CODE OF PRACTICE ON COVERT SURVEILLANCE AND PROPERTY INTERFERENCE 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;
"ANPR" means automatic number plate recognition;
"CCTV" means closed-circuit television;

(**a**) Ordinance 26/2012

"CHIS" means a covert human intelligence source;
"CI authorisation" has the meaning given in section 6 of RIPO;
"confidential information" means confidential journalistic information, confidential personal information and matters subject to legal privilege;
"confidential journalistic information" has the meaning given in section 7 of RIPO;
"confidential personal information" has the meaning given in section 8 of RIPO;
"ECHR" means the European Convention for the Protection of Human Rights and Fundamental Freedoms;
"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;
"LC authorisation" has the meaning given in section 11 of RIPO;
"matters subject to legal privilege" has the meaning given in section 13 of RIPO;
"private information" has the meaning given in section 3(1) of RIPO;
"relevant crime" has the meaning given in section 3(1) of RIPO;
"RIPO" means the Regulation of Investigatory Powers Ordinance 2012 as amended and updated from time to time;
"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 covert surveillance that is likely to result in the obtaining of private information about a person and the authorisation of the entry on or interference with property 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 covert surveillance that is likely to result in the obtaining of private information about a person or to authorise entry on or interference with property.

1.5. Note that where covert surveillance activities are unlikely to result in the obtaining of private information about a person, or where there is a separate legal basis for such activities, this, or any, code need not apply.

Effect of code

1.6. 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

a P.I. 28/2012

use or granting of authorisations in general or the failure to use or grant authorisations where appropriate.

1.7. Examples are included in this code to assist with the illustration and interpretation of certain provisions. Examples are 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.

Surveillance activity to which this code applies

1.8. RIPO provides for the authorisation of covert surveillance by investigating authorities within the territorial boundaries of the SBAs where that surveillance is likely to result in the obtaining of private information about a person.

1.9. Surveillance, for the purpose of RIPO, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of anything monitored, observed or listened to in the course of the surveillance.

1.10. RIPO uses the term "covert surveillance". Surveillance is "covert" only if it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place, is carried out in relation to a specific investigation or operation and in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under RIPO).

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

Basis for lawful surveillance activity

1.12. The Human Rights Ordinance 2004 gives effect in domestic law to certain rights set out in the ECHR. Some of the rights conferred are absolute, such as the prohibition on torture, while others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied.

1.13. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR. It is Article 8 that is most likely to be engaged when investigating authorities seek to obtain private information about a person by means of covert surveillance.

1.14. Article 6 of the ECHR, the right to a fair trial, may also be engaged where a prosecution follows an investigation involving the use of covert techniques, particularly where defence counsel seek disclosure in order to challenge the

lawfulness of an authorisation and/or the prosecution seek to protect the use of those techniques through public interest immunity procedures.

1.15. RIPO provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8. However, where such surveillance would not be likely to result in the obtaining of any private information about a person, no interference with Article 8 rights should occur, and an authorisation under RIPO is therefore not appropriate.

1.16. Similarly, an authorisation under RIPO is not required if the SBA Police or other investigating authority has another clear legal basis for conducting covert surveillance likely to result in the obtaining of private information about a person which satisfies the requirements of Article 8.

1.17. Chapter 2 provides further guidance on what constitutes private information and examples of activity for which authorisations under RIPO are or are not required.

Investigating authorities

1.18. Only two investigating authorities may apply for authorisations under RIPO - the SBA Police and the SBA Customs & Immigration Service.

International considerations

1.19. Authorisations under RIPO can be granted only for surveillance carried out within the territorial jurisdiction of the SBAs. Cross border arrangements for covert surveillance between the SBAs, the Republic of Cyprus or the areas of the Republic of Cyprus not under the effective control of the government of the Republic of Cyprus do not currently exist.

2.0 Covert surveillance definitions

2.1. This chapter provides further guidance on whether surveillance activity is covert surveillance, or where an authorisation for activity may not be required under RIPO.

2.2. Surveillance is covert surveillance if the following are <u>all</u> true:

- it is undertaken in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place;
- it is conducted for the purposes of a specific investigation or operation;
- it is likely to result in the obtaining of private information about a person (whether or not a person specifically identified for the purposes of the investigation or operation);
- it is undertaken otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPO to be sought.

2.3. An authorisation under RIPO cannot be granted for covert surveillance that consists of intercepting a communication in the course of transmission by means of a postal service or telecommunications system.

2.4. An authorisation under RIPO cannot be granted for covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device that is present on the premises or in the vehicle. Nor may an authorisation be granted for covert surveillance that takes place by means of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as might be expected to be obtained from a device inside.

Private information

2.5. RIPO states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

2.6. Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by investigating authorities of that person's activities for future consideration or analysis. A person in custody will have certain expectations of privacy.

Example 1: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A covert surveillance authorisation would therefore be appropriate for investigating authorities to record or listen to the conversation as part of a specific investigation or operation and otherwise than by way of an immediate response to events.*

2.7. Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or some cases overtly) obtained for purposes of making a permanent record on that person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a covert surveillance authorisation may be required.

Example 2: *Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a covert surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a covert surveillance authorisation should be considered.*

2.8. Private information may include personal data, such as name, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a covert surveillance authorisation is appropriate.

Example 3: *An officer conducting surveillance intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A covert surveillance authorisation should therefore be sought.*

Use of tracking devices

2.9. The use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle or a particular item, for example, a piece of plant machinery, alone do not necessarily constitute covert surveillance as they do not necessarily provide private information about any individual, but sometimes only supply information about the location of that particular device at any one time. However, the subsequent use of that information, coupled with other surveillance activity which may obtain private information, could interfere with Article 8 rights. An authorisation for covert surveillance may therefore be appropriate.

(The use of such devices is also likely to require an authorisation for property interference.)

Recording of telephone conversations

2.10. An authorisation under RIPO cannot be granted for covert surveillance that consists of intercepting a communication in the course of transmission by means of a postal service or a telecommunications system.

2.11. However, the recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised covert surveillance operation will not constitute interception of communications provided the process by which the content of the communication is obtained during the course of its transmission does not involve any modification of, or interference with, the telecommunications system or its operation. A telecommunications system begins at the point at which the sound waves representing the conversation reach the telephone handset and are converted to an electrical impulse or signal for onward transmission through the system. The recording or monitoring of one or both ends of a telephone conversation by a surveillance device will not therefore constitute interception, as sound waves obtained from the air are not in the course of transmission by means of a telecommunications system (which, in the case of a telephone conversation, should be taken to begin with the microphone and end with the speaker). Any such product can be treated as having been lawfully obtained.

Example 4: *An officer engaged on an operation authorised for covert surveillance is able to get so close to the subject in a restaurant that he can hear and record any conversations made by the subject on his mobile telephone. If one or both ends of a telephone conversation made are recorded during the course of the operation, this will not constitute unlawful interception provided the recording device obtains the product from the sound waves in the restaurant and not by interference with, or modification of, any part of the telecommunications system.*

Residential premises and private vehicles

2.12. An authorisation under RIPO cannot be granted for covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device that is present on the premises or in the vehicle. Nor may an authorisation be granted for covert surveillance that takes place by means of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as might be expected to be obtained from a device inside.

2.13. For the purposes of RIPO, residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. This specifically includes hotel, prison and custody accommodation that is so occupied or used. However, common areas (such as hotel dining areas) to which a person has

access in connection with their use or occupation of accommodation are specifically excluded.

2.14. RIPO further states that the concept of premises should be taken to include any place whatsoever, including any vehicle or moveable structure, whether or not occupied as land.

2.15. Examples of residential premises would therefore include:

- a rented flat currently occupied for residential purposes;
- a prison cell (or police cell serving as temporary prison accommodation);
- a hotel bedroom or suite.

2.16. Examples of premises which would not be regarded as residential would include:

- a communal stairway in a block of flats (unless known to be used as a temporary place of abode by, for example, a homeless person);
- a prison canteen or police interview room;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public.

2.17. A private vehicle is defined in RIPO as any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.

2.18. Covert surveillance is not able to be authorised, if it is carried out by means of a surveillance device placed outside residential premises or private vehicles, if the device consistently provides information of the same quality and detail as might be expected to be obtained from a device inside.

Example 5: *An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute surveillance that cannot be authorised. However, a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute surveillance that cannot be authorised.*

2.19. The use of a device for the purpose of providing information about the location of a private vehicle may be authorised under RIPO where the recording or use of the information about the location of the vehicle would amount to the covert monitoring of the movements of the occupant(s) of the vehicle. A property interference authorisation may be appropriate for the covert installation or deployment of the device.

Places set aside for legal consultations

2.20. See paragraphs 4.12 to 4.16.

Where authorisation is not required

2.21. Some covert activity does not constitute covert surveillance for the purposes of RIPO and a covert surveillance authorisation is not appropriate. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not for the purposes of a specific investigation or a specific operation;
- overt use of CCTV and ANPR systems;
- certain other specific situations.

2.22. Each situation is detailed and illustrated below.

Immediate response

2.23. Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to sudden and unforeseeable events, such that it is not reasonably practicable to obtain an authorisation under RIPO, does not require a covert surveillance authorisation.

Example 6: *An authorisation under RIPO is not appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol or monitor social media accounts during a public order incident .*

General observation activities

2.24. The general observation duties of many police and other law enforcement officers do not require authorisation under RIPO, whether covert or overt. Such general observation duties frequently form part of the statutory functions of investigating authorities against breaches of law and order, as opposed to the pre-planned surveillance of a specific person or group of people. Wherever these activities are unlikely to result in the obtaining of private information about a person, a covert surveillance authorisation is not appropriate.

Example 7: *Plain clothes police officers on patrol to monitor a crime hot-spot or prevent and detect car theft would not require a covert surveillance authorisation. Their objective is merely to observe a location and to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance, and the obtaining of private information is unlikely. A covert surveillance authorisation is not available.*

Example 8: *Police officers monitoring a car boot sale where it is suspected that counterfeit goods are being sold. Again, this is part of the general duties of investigating authorities, and the likelihood of obtaining private information about any person is negligible.*

Example 9: *Police officers carrying out surveillance intend to follow and observe Z covertly as part of a pre-planned operation to determine their suspected involvement in car theft. It is proposed to conduct covert surveillance of Z and record Z's activities as part of the investigation. In this case, private life considerations are likely to arise, and a covert surveillance authorisation should be sought.*

Example 10: *Police officers monitoring publicly accessible information on social media websites, using a general search term (such as the name of a particular event they are policing), would not normally require a directed surveillance authorisation. However, if they were seeking information relating to a particular individual or group of individuals, for example, by using the search term "group x" (even where the true identity of those individuals is not known) this may require authorisation. This is because use of such a specific search term indicates that the information is being gathered as part of a specific investigation or operation, particularly in circumstances where information is recorded and stored for future use.*

Not relating to specified grounds or core functions

2.25. An authorisation for covert surveillance is not available if the surveillance is undertaken other than for the purposes of a "specific investigation or a specific operation". Covert surveillance for any other general purposes should be conducted under other powers.

2.26. Covert surveillance is carried out by investigating authorities which are responsible for the discharge of specific public functions and are equipped with investigatory powers for the performance of those functions. In the United Kingdom case of C v. the Police and the Secretary of State for the Home Department (case no. IPT/03/32/H dated 14 November 2006), the United Kingdom Investigatory Powers Tribunal held that directed surveillance (the term used in the United Kingdom legislation) under Part 2 of the Regulation of Investigatory Powers Act 2000 (UK) was limited:

". . . to the discharge of the public authority's particular public or "core function" specific to it, rather than the carrying out of "ordinary functions" common to all investigative authorities, such as employment (or its nearest equivalent in the case of the police) and entering into contracts to receive or supply other services."

2.27. In practice, this means that an authorisation is only available in respect of the carrying out of the "specific public functions" undertaken by a particular authority, in contrast to the "ordinary functions" which are those undertaken by all authorities (e.g.,

employment issues, contractual arrangements, etc.). The disciplining of an employee is not usually a "core function", although it may be if it relates to a criminal offence. For example, if a police employee was suspected by the force of criminal activities in the course of his work or activity then an authorisation for covert surveillance may be available.

Example 11: *A police officer is suspected by the force of undertaking additional employment in breach of discipline regulations. The SBA Police wish to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute covert surveillance for the purposes of RIPO as it does not relate to the discharge of the police force's core functions and is not therefore being undertaken for the purposes of a "specific investigation or a specific operation". It relates instead to the carrying out of ordinary functions, such as employment, which are common to all investigating authorities. Activities of this nature are covered by the employment relationship.*

CCTV and ANPR systems

2.28. The use of overt CCTV cameras by does not normally require an authorisation under RIPO. Members of the public will be aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under RIPO.

Example 12: *There may be circumstances where overt surveillance equipment, such as shopping centre CCTV system, is used to gather information as part of a reactive operation (e.g., attempts to identify offenders for criminal damage offences in a town centre or shoplifting). This may not necessarily amount to covert surveillance if the persons subject to the surveillance are aware that it is taking place. Use in these circumstances is unlikely to interfere with Article 8 rights and is generally no more than an intelligence-driven use of the crime prevention and detection capability of CCTV.*

2.29. However, where CCTV or ANPR cameras are used in a covert and pre-planned manner for the surveillance of a specific person or group of people, a covert surveillance authorisation should be considered. Such covert surveillance forms part of a specific investigation or operation and may result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of covert surveillance. The use of the CCTV or ANPR system in these circumstances goes beyond their intended use for the general prevention and detection of crime and protection of the public.

Example 13: *A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a community area. A decision is taken to use the local CCTV system to conduct surveillance against that individual such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt local CCTV system to monitor and/or record that individual's movements should be considered for a covert surveillance authorisation.*

Specific situations not requiring covert surveillance authorisation

2.30. The following specific activities constitute neither directed nor intrusive surveillance:

- The use of a recording device by a CHIS who has been properly tasked to record any information which is disclosed in his presence does not constitute covert surveillance and therefore an authorisation for covert surveillance under RIPO cannot be granted. An authorisation for the conduct or the use of a CHIS should be considered.
- The covert recording of suspected noise nuisance where the intent is only to record excessive noise levels from premises and the recording device is calibrated to record only excessive noise levels. In such circumstances, the perpetrator would normally be regarded as having forfeited any claim to privacy and an authorisation may not be necessary.
- the recording, whether overt or covert, of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a member of an investigating authority. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a member of an investigatory authority and that information gleaned through the interview has passed into the possession of the investigatory authority in question.

3.0 General rules on authorisations

Overview

3.1. An authorisation under RIPO will, providing the statutory tests are met, provide a lawful basis for investigating authorities to carry out covert surveillance activity that is likely to result in the obtaining of private information about a person. Responsibility for granting authorisations varies depending on the nature of the operation.

Necessity and proportionality

3.2. RIPO stipulates that the person granting an authorisation for covert surveillance, or for the entry on or interference with property, must be satisfied that the activities to be authorised are necessary on one or more statutory grounds.

3.3. If the activities are deemed necessary on one of more of the statutory grounds, the person granting the authorisation must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the target 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 to be conducted 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 intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could be reasonably obtained by other less intrusive means.

3.5. The following points should therefore be addressed when considering whether the authorised conduct is proportionate to what is sought to be achieved by carrying it out:

- 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 had been considered and why they were not implemented.

3.6. It is important, therefore, that all those involved in undertaking covert surveillance activities or the entry on or interference with property under RIPO are fully aware of the extent and limits of the authorisation in question.

Example 14: *An individual is suspected of carrying out a series of minor criminal damage offences at a local shop following a dispute with the owner. It is suggested that a period of pre-planned covert surveillance should be conducted to record the individual's movements and activities on the basis that the authorisation is necessary for the purpose of preventing or detecting imprisonable crime. Although preventing and detecting imprisonable crime is, in principle, a legitimate ground on which a covert surveillance authorisation may be granted, it is unlikely that the resulting interference with privacy will be necessary or proportionate in the circumstances of the particular case. In particular, the obtaining of private information on the individual's daily routine (and potentially that of innocent third parties with whom he associated) is unlikely to be required in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.*

Example 15: *An individual is suspected of a relatively minor offence, for example, unlawful gambling. It is suggested that a covert surveillance authorisation should be obtained in order to record his movements and activities for the purpose (as relevant) of preventing or detecting imprisonable crime. Although this is a legitimate ground on which a covert surveillance authorisation may be granted, the tests of necessity and proportionality will not be satisfied in the circumstances of this particular case and the nature of the surveillance to be conducted. In particular, the obtaining of private information on the individual's daily routine and potentially of innocent third parties with whom he associates is unlikely to be required in order to investigate the activity of concern. Instead, readily available and less intrusive measures should be considered, such as general observation of the location in question until such time as a crime may be committed. In addition, it is likely that such offences can be tackled using overt techniques.*

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

Collateral intrusion

3.8. Before authorising applications for covert surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not subjects of the surveillance (collateral intrusion).

3.9. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities

may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion.

3.10. All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions.

Example 16: *SBA Customs & Immigration seeks to conduct covert surveillance against T on the grounds that this is necessary and proportionate for the investigation of offences connected with illegal immigration. It is assessed that such surveillance will unavoidably result in the obtaining of some information about members of T's family, who are not the intended subjects of the surveillance. 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. This may include not recording or retaining any material obtained through such intrusion.*

3.11. Note that where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion. Any such surveillance activity should be carefully considered against the necessity and proportionality criteria as described above (paragraphs 3.2 to 3.6).

Example 17: *The police seek to conduct a covert surveillance operation to establish the whereabouts of N in the interests of preventing a serious crime. It is proposed to conduct covert surveillance against P, who is an associate of N but who is not assessed to be involved in the crime, in order to establish the location of N. In this situation, P will be the subject of the covert surveillance authorisation and the authorising officer should consider the necessity and proportionality of conducting covert surveillance against P, bearing in mind the availability of any other less intrusive means to identify N's whereabouts. It may be the case that covert surveillance of P will also result in obtaining information about P's family, which in this instance would represent collateral intrusion also to be considered by the authorising officer.*

3.12. In order to give proper consideration to collateral intrusion, an authorising officer or person considering issuing the warrant should be given full information regarding the potential scope of the anticipated surveillance or interference, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the authorising officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The authorising officer or person considering

issuing the warrant should ensure appropriate safeguards for the handling, retention or destruction of such material in accordance with chapter 8 of this code, as well as compliance with data protection requirements.

3.13. Where an investigating authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

Example 18: *If an individual provides the police with passwords and log-in details for their personal social networking accounts in order to provide evidence of threats made against them, this would not normally require a directed surveillance authorisation. If the police then decided to monitor the accounts for the purposes of obtaining further evidence of criminal activity by the author of the threats, they should consider applying for a directed surveillance authorisation in circumstances where private information is likely to be obtained. This is because the police would be acting with the intention to monitor an individual who has not consented to and may not be aware of the surveillance. The public authority will also need to consider the extent of the collateral intrusion into the privacy of others who may comment on or post information onto the accounts under surveillance.*

Reviewing authorisations

3.14. Regular reviews of all authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be retained for at least 3 years (see Chapter 7). Particular attention is drawn to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or significant collateral intrusion, or confidential information is likely to be obtained.

3.15. In each case the frequency of reviews should be considered at the outset by the authorising officer. This should be as frequently as is considered necessary and practicable.

3.16. The authorising officer must assess whether the authorisation should continue or whether the criteria on which he based the original decision have changed sufficiently to cause a revocation of the authorisation. Support staff can do the necessary research and prepare the review process, but the actual review is the responsibility of the original authorising officer and should, as a matter of good practice, be conducted by him or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms.

3.17. Any proposed or unforeseen changes to the nature or extent of the surveillance operation that may result in further or greater intrusion into the private life of any

person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion), before approving or rejecting them. Any such changes must be highlighted at the next renewal if the authorisation is to be renewed.

3.18. Where a covert surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if the authorisation is to be renewed.

> ***Example 19:*** *A covert surveillance authorisation is obtained by the police to authorise surveillance of "X and his associates" for the purposes of investigating their suspected involvement in a crime. X is seen meeting with A in a café and it is assessed that subsequent surveillance of A will assist the investigation. Surveillance of A may continue (he is an associate of X) but the covert surveillance authorisation should be amended at a review to include "X and his associates, including A".*

3.19. During a review, the reviewing officer may cancel aspects of the authorisation, for example to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

Combined authorisations

3.20. A single authorisation may combine any number of authorisations under RIPO. However, the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer.

3.22. The above considerations do not preclude investigating authorities from obtaining separate authorisations. Where separate authorisations are sought, consideration should be given to whether reference to these in the related warrants or authorisations is appropriate.

General best practice

3.23. The following are not statutory requirements or formal provisions of this code, but should be considered as best working practices by investigating authorities with regard to all applications for authorisations covered by this code:

- applications should avoid any repetition of information;
- information contained in applications should be limited to that required by RIPO;
- the case for the authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take

account of information which support or weakens the case for the warrant or authorisation;

- where an authorisation is granted orally under urgency procedures (see Chapter 5 on authorisation procedures), section 25(3) of RIPO states that it must be recorded in writing as soon as reasonably practicable thereafter. Best practice suggests that, where possible, both the applicant and the authorising officer in such cases make a contemporaneous note. The note should include the intelligence case, the time of the application and the authorisation, and the precise action authorised.
- an application should not require the sanction of any person in the police or other investigating authority other than the authorising officer;
- where it is foreseen that other authorities will be involved in carrying out the surveillance, these authorities should be detailed in the application;
- authorisations should not generally be sought for activities already authorised following an application by the same or different authority.

3.24. It is considered good practice that within every investigatory public authority, a senior responsible officer should be responsible for:

- the integrity of the process in place within the investigating authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
- compliance with RIPO;
- oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections; and
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

Online covert activity

3.25. The growth of the internet, and the extent of the information that is now available online, presents new opportunities for investigating authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other functions, as well as in understanding and engaging with the public they serve. It is important that investigating authorities are able to make full and lawful use of this information. Much of it can be accessed without the need for RIPO authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPO authorisations may need to be considered. The following guidance is intended to assist investigating authorities in identifying when such authorisations may be appropriate.

3.26. The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private

information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of an investigating authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.24 to 4.29 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

3.27. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where an investigating authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

3.28. As set out in paragraph 3.29 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

3.29. Where information about an individual is placed on a publicly accessible database, for example the telephone directory, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Example 20: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.*

Example 21: *A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 22: *An investigating authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPO authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.*

3.30. Whether an investigating authority interferes with a person's private life includes a consideration of the nature of the investigating authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where an investigating authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

3.31. In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;

- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

3.32. Internet searches carried out by a third party on behalf of an investigating authority, or with the use of a search tool, may still require a directed surveillance authorisation.

Example 23: *Researchers within an investigating authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.*

Aerial covert surveillance

3.33. Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, the same considerations of this code should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

Example 24: *An unmanned aircraft deployed by the police to monitor a subject of interest at a public demonstration is likely to require an authorisation for directed surveillance, as it is likely that private information will be obtained and those being observed are unaware it is taking place, regardless of whether the drone is marked as belonging to the police force. Unless sufficient steps have been taken to ensure that participants in the demonstration are aware that aerial surveillance will be taking place, such activity should be regarded as covert.*

4.0 Confidential information

Overview

4.1. Confidential information is a term used in this code to refer to matters subject to legal privilege, confidential personal information and confidential journalistic material. RIPO does not provide special protection for confidential information except in the case of "CI authorisations". These are authorisations for the entry on or interference with property that are likely to result in confidential information being acquired. CI authorisations require (other than in urgent cases) the approval of the IPC before they take effect.

4.2. In addition, special provision is made for authorisations for covert surveillance in certain locations where legal consultations and certain medical consultations for legal purposes are taking place – "LC authorisations". LC authorisations (other than in urgent cases) require the approval of the IPC before they take effect.

4.3. Even when RIPO provides no special protection for confidential information, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. So, for example, extra care should be taken where, through the use of surveillance, it is likely that knowledge will be acquired of communications between a minister of religion and an individual relating to the latter's spiritual welfare, or wherever matters of medical or journalistic confidentiality or matters subject to legal privilege may be involved.

Material subject to legal privilege: introduction.

4.4. Covert surveillance likely or intended to result in the acquisition of knowledge of matters subject to legal privilege may take place in the context of an LC authorisation or may take place in other circumstances. Similarly, property interference may take place in circumstances where knowledge of matters subject to legal privilege is likely to be obtained.

4.5. "Matters subject to legal privilege" is defined in section 13 of RIPO. This definition should be used to determine how to handle material obtained through surveillance under RIPO. 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 there are grounds to believe, for example, that 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.

Tests to be applied when authorising or approving covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege

4.6. All applications for covert surveillance or property interference that may result in the acquisition of knowledge of matters subject to legal privilege should state whether the covert surveillance or property interference is intended to obtain knowledge of matters subject to legal privilege as defined in section 13 of RIPO.

4.7. If the covert surveillance or property interference 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 identify all steps which will be taken to mitigate the risk of acquiring it. If the risk cannot be removed entirely, the application should explain what steps will be taken to ensure that any knowledge of matters subject to legal privilege which is obtained is not used in law enforcement investigations or criminal prosecutions.

4.8. Where covert surveillance or property interference is likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, an authorisation must only be granted or approved if the authorising officer or IPC, as appropriate, is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary:

- where the surveillance or property interference is not intended to result in the acquisition of knowledge of matters subject to legal privilege, such exceptional and compelling circumstances may arise for the purpose of preventing or detecting serious crime;
- where the surveillance or property interference is intended to result in the acquisition of knowledge of matters subject to legal privilege, 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 surveillance or property interference is reasonably regarded as likely to yield intelligence necessary to counter the threat.

4.9 Further, in considering any authorisation for covert surveillance or property interference likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, the authorising officer or IPC, as appropriate, must be satisfied that the proposed covert surveillance or property interference is proportionate to what is sought to be achieved.

4.10. Authorisations for covert surveillance likely to result in the acquisition of knowledge of matters subject to legal privilege may be granted only by the Chief Constable or Fiscal Officer (or other authorising officers in urgent cases). LC authorisations are subject to prior approval by the IPC (unless the case is urgent).

4.11. Authorisations for the entry on or interference with property likely to result in the acquisition of such material are subject to prior approval by the IPC (unless the case is urgent) - see paragraphs 4.17 to 4.20.

Covert surveillance of places set aside for legal consultations - LC authorisations

4.12. RIPO provides that covert surveillance that is carried out in relation to anything taking place on so much of any premises specified in section 11(2) of RIPO as is, at any time during the surveillance, used for the purpose of a legal consultation is an "LC consultation".

4.13. The premises are:

- a police station;
- a customs station (designated under section 9 of the Customs Ordinance 2005);
- the place of business of a professional legal adviser;
- a prison or other place in which persons serving sentences of imprisonment or being held in custody may be detained; and
- a place used for the sittings and business of any court, tribunal, inquest or inquiry.

4.14. A "legal consultation" means:

- a consultation between a professional legal adviser and the legal adviser's client or any person representing the client; or
- a consultation between a medical practitioner and a professional legal adviser, the legal adviser's client or any person representing the client that is made in connection with or in contemplation of legal proceedings and for the purpose of such proceedings.

4.15. The definition of "legal consultation" does not distinguish between legal consultations which are legally privileged, wholly or in part, and legal consultations which may be in furtherance of a criminal purpose and are therefore not protected by legal privilege. Covert surveillance of all legal consultations set out above are LC authorisations (whether protected by legal privilege or not) and are subject to the requirements referred to in paragraph 4.16.

4.16. LC authorisations may be granted only for the purpose of preventing or detecting serious crime. Except in urgent cases, LC authorisations do not take effect until such time as:

- the authorisation has been approved by the IPC; and
- written notice of the IPC's decision to approve the authorisation has been given to the authorising officer.
-

Property interference likely to result in the acquisition of matters subject to legal privilege, confidential personal information and confidential journalistic material - CI authorisations

4.17. An authorisation for the entry on or interference with property is a "CI authorisation" if, at the time it is granted, the authorising officer believes that the conduct authorised by it is likely to result in any person acquiring knowledge of

matters subject to legal privilege, confidential personal information or confidential journalistic material.

4.18. 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.

4.19. 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.

4.20. With the exception of urgent authorisations, a CI authorisation does not take effect until such time as:

- the authorisation has been approved by the IPC; and
- written notice of the IPC's decision to approve the authorisation has been given to the authorising officer.

The use and handling of matters subject to legal privilege

4.21. Matters subject to legal privilege are particularly sensitive, and surveillance which acquires such material may give rise to issues under Article 6 of the ECHR (right to a fair trial) as well as engaging Article 8.

4.22. Where investigating authorities deliberately acquire knowledge of matters subject to legal privilege, they may use that knowledge to counter the threat which led them to acquire it, but it will not be admissible in court. Investigating authorities should ensure that knowledge of matters subject to legal privilege, whether or not it is acquired deliberately, is kept separate from law enforcement investigations or criminal prosecutions.

4.23. In cases likely to result in the acquisition 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 legally privileged material has been acquired 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).

4.24. 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.

4.25. Where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, advice should be sought from AGLA's Office before any further dissemination of the information takes place. Advice should also be sought from AGLA's Office where there is doubt over whether information is not subject to legal privilege due to the "in furtherance of a criminal purpose" exception.

4.26. The retention of legally privileged material, 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.

The use and handling of other confidential information

4.27. Special consideration must also be given to authorisations that involve 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 made available if requested.

4.28. 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.

5.0 Authorisation procedures for covert surveillance

Authorisation criteria

5.1. Under RIPO an authorisation for covert surveillance may be granted by an authorising officer where he is satisfied that the authorisation is necessary:

- in the case of an LC authorisation, for the purpose of preventing or detecting serious crime;
- in the case of any other authorisation,

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

5.2. The authorising officer must also be satisfied that the surveillance is proportionate to what it seeks to achieve (see paragraphs 3.2 to 3.6).

Authorisation procedures

5.3. Responsibility for authorising the carrying out of covert surveillance rests with the authorising officer and requires the personal authority of the authorising officer. RIPO designates the rank of the authorising officer necessary for a particular type of authorisation and the officers entitled to act in urgent cases.

5.4. The authorising officer must grant authorisations in writing. However, in urgent cases 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 record that the authorising officer has expressly authorised the action should be made in writing by both the authorising officer and the applicant as soon as is reasonably practicable, together with the information detailed in paragraph 5.9.

5.5. A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer is available to grant the authorisation would, in the judgement of the person granting the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being granted. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's or applicant's own making.

5.6. Authorising officers should not be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises such an investigation or operation, the centrally retrievable record of authorisations (see Chapter 7) should highlight this, and the attention of the IPC should be drawn to it during the next inspection.

5.7. 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 other customs officers.

Information to be provided in applications for authorisation.

5.8. A written application for a covert surveillance authorisation should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and the grounds (e.g., for the purpose of preventing or detecting imprisonable crime) listed in RIPO;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- 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 surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authorisation was granted or refused, by whom and the time and date this happened.

5.9. In urgent cases, the above information may be supplied orally. In such cases, the authorising officer and applicant, where applicable, should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

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

Duration of authorisations

5.10. A written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of 3 months beginning with

the day on which it took effect. So an authorisation granted at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day.) Even in instances where it is anticipated that an authorisation will only be required for a period of time less than three months, authorisation should still be granted for the three month period, subject to review at an interval reflecting expected duration, and the authorisation cancelled when it is no longer necessary.

5.11. Urgent oral authorisations or written authorisations granted 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.

Renewals

5.12. If, at any time before an authorisation for covert surveillance 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 3 months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours. The renewal will take effect at the time at which, or day on which, the authorisation would have ceased to have effect but for the renewal.

5.13. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

5.14. All applications for the renewal of a covert surveillance authorisation should record (at the time of application, or when reasonably practicable in the case of urgent cases approved orally):

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information in paragraph 5.8;
- the reasons why the authorisation for covert surveillance should continue;
- the content and value to the investigation or operation of the information so far obtained by the surveillance; and
- the results of regular reviews of the investigation or operation.

5.15. Authorisations may be renewed more than once, if necessary, and the details of the renewal should be centrally recorded (see Chapter 7).

Cancellations

5.16. During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease surveillance against one of a number of named subjects or to discontinue the use of a particular tactic. He must cancel the authorisation if satisfied that the covert surveillance as a whole no longer meets the criteria upon which it was authorised. Where the original 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.

5.17. As soon as the decision is taken that covert surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained (see Chapter 7). There is no requirement for any further details to be recorded when cancelling a covert surveillance authorisation. However, effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved, and a direction given as to the retention and/or destruction of records.

6.0 Authorisation procedures for entry on or interference with property

Need for authorisations

6.1. Authorisations under RIPO should be sought wherever members of an investigating authority, or persons acting on their behalf, enter on or interfere with property, in circumstances where the entry or interference would otherwise be unlawful.

6.2. In many cases an operation using covert techniques may involve covert surveillance and the entry on or interference with property. This can be done as a combined authorisation, although the criteria for authorisation of each activity must be considered separately.

6.3. An entry on or interference with property authorisation is not required for entry (whether for the purpose of covert recording or for any other legitimate purpose) into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are afforded unqualified access. Nor is authorisation required for entry on property, such as land or premises at the invitation of the occupier. This is so whatever the purposes for which the premises are used. However, if the consent for entry has been obtained by deception (e.g., requesting entry for a false purpose), an authorisation for entry on land should be obtained.

Informed consent

6.4. Authorisations under RIPO are not necessary where the investigating authority is acting with the informed consent of a person able to give permission in respect of the relevant property and actions. However, consideration should still be given to the need to obtain a covert surveillance authorisation, depending on the operation.

Incidental property interference

6.5. RIPO provides that no person is to be subject to any civil liability in respect of any conduct which is incidental to correctly authorised covert surveillance activity and is not itself conduct for which a separate authorisation might reasonably have been expected to have been sought under RIPO. Thus a person is not, for example, subject to civil liability for trespass where that trespass is incidental to properly authorised covert surveillance activity and where an authorisation for entry on or interference with property is available but might not reasonably have been expected to be sought (perhaps due to the unforeseeable nature or location of the activity).

> ***Example 18:*** *Officers crossing an area of land covered by an authorisation under RIPO are forced to temporarily and momentarily cross into neighbouring land to bypass an unforeseen obstruction, before returning to their authorised route.*

6.6. Where an investigating authority is capable of obtaining an authorisation for incidental conduct, it should seek one wherever it could be reasonably expected to do so.

Samples

6.7. The acquisition of samples, such as DNA samples, fingerprints and footwear impressions, where there is no consequent loss of or damage to property does not of itself constitute unlawful property interference. However, wherever it is necessary to conduct otherwise unlawful property interference to access and obtain these samples, an authorisation under RIPO would be appropriate. An authorisation for covert surveillance would not normally be relevant to any subsequent information, whether private or not, obtained as a result of the covert technique. Once a DNA sample, fingerprint or footwear impression has been obtained, any subsequent analysis of this information will not be surveillance as defined in section 10(2) of RIPO.

Example 26: *Police wish to take fingerprints from a public telephone to identify a suspected criminal who is known recently to have used the telephone. The act of taking the fingerprints would not involve any unlawful property interference so no authorisation under RIPO is required. The subsequent recording and analysis of the information obtained to establish the individual's identity would not amount to surveillance and therefore would not require authorisation under RIPO.*

Example 27: *Police intend to acquire covertly a mobile telephone used by a suspected criminal, in order to take fingerprints. In this case, the acquisition of the telephone for the purposes of obtaining fingerprints could be authorised under RIPO where it would otherwise be unlawful.*

Authorisations for entry on or interference with property by investigating authorities

6.8. Responsibility for these authorisations rests with the authorising officer as defined in RIPO. Authorisations require the personal authority of the authorising officer except in urgent situations, where it is not reasonably practicable for the application to be considered by such person. The person entitled to act in such cases is set out in RIPO.

6.9. Authorisations for the entry on or interference with property may be granted under sections 22 (preventing or detecting serious crime) and 23 (preventing or detecting relevant crime).

6.10. An authorisation under section 22 may be granted for the purposes of, or in connection with, the carrying out of covert surveillance or for purposes unrelated to covert surveillance. However, if it is granted for the purposes of, or in connection with, the carrying out of covert surveillance, the covert surveillance must have been authorised under section 20 of RIPO.

6.11. An authorisation for the entry on or interference with property under section 23 may be granted only for the purposes of, or in connection with, the carrying out of covert surveillance authorised under section 20 of RIPO. However, if the

authorisation is a CI authorisation, an authorisation under section 23 is not available, and an authorisation under section 22 (if available) must be obtained.

6.12. Section 22 provides that an authorising officer may grant an authorisation for the entry on or interference with property if the officer is satisfied that—

- consideration has been given as to whether it would be reasonably practicable, without prejudicing the investigation or operation, to obtain permission to enter on or interfere with the property;
- the authorisation is necessary for the purpose of preventing or detecting serious crime; and
- the authorised entry or interference with property is proportionate to what is sought to be achieved by undertaking it. The authorising officer must take into account whether what is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

6.13. Section 23 provides that an authorising officer may grant an authorisation (referred to as the "second authorisation") for the entry on or interference with property if the officer is satisfied that—

- the conduct authorised by the second authorisation is for the purposes of, or in connection with, the carrying out of covert surveillance specified in an authorisation under section 20 (the "first authorisation") and for no other purpose;
- the second authorisation is not a CI authorisation;
- consideration has been given as to whether it would be reasonably practicable, without prejudicing the investigation or operation, to obtain permission to enter on or interfere with the property;
- both the first and the second authorisations are necessary for the purpose of preventing or detecting relevant crime; and
- the authorised entry or interference with property is proportionate to what is sought to be achieved by undertaking it. The authorising officer must take into account whether what is thought necessary to achieve by the authorised conduct could reasonably be achieved by other means.

6.14. Conduct that may be authorised under section 23 includes—

- entering and remaining on land;
- placing a surveillance device on or in, or attaching such a device to,—
  (i) land which the authorisation gives power to enter or anything attached to such land;
  (ii) a vehicle or other item on or in a public place, land which the authorisation gives power to enter or other land to enter which permission has been obtained or is implied;
- using, maintaining and retrieving a surveillance device.

6.15. Section 20 provides restrictions on the covert surveillance that may be authorised under RIPO (see paragraphs 2.3 and 2.4). Accordingly, authorisations for

the entry on, or interference with property, may not be granted for the purposes of carrying out covert surveillance that may not be authorised under RIPO.

6.16. Further, an authorisation under section 22 or 23 may not be granted to enter residential premises, a building, land covered by a building or land within the curtilage of a building. RIPO defines "building" so as to exclude a partially-constructed structure that is unused.

Authorisation procedures

6.17. Authorisations will generally be granted by the authorising officer in writing. However, in urgent cases, they may be granted orally by an authorising officer whose entitlement to act is not confined to urgent applications. In such cases, a statement that the authorising officer has expressly authorised the action(s) should be recorded in writing by the applicant as soon as is reasonably practicable, together with the information detailed in paragraph 6.20.

6.18. If the authorising officer is absent, an authorisation can be granted in writing in urgent cases by the officer entitled to act in urgent cases, as provided for in RIPO.

Information to be provided in applications

6.19. Applications to the authorising officer for the granting or renewal of an authorisation must be made in writing (unless urgent) by a police officer or customs officer and should specify:

- the identity or identities, where known, of those who possess the property that is to be subject to the entry or interference;
- sufficient information to identify the property which the entry or interference will affect;
- the nature and extent of the proposed entry or interference;
- the details of any collateral intrusion, including the identity of individuals and/or categories of people, where known, who are likely to be affected, and why the intrusion is justified;
- details of the offence suspected or committed;
- how the authorisation criteria have been met;
- any action which may be necessary to maintain any equipment (including replacing it);
- any action which may be necessary to retrieve any equipment;
- details of the consideration given to whether it would be reasonably practicable, without prejudicing the investigation or operation, to obtain permission to enter or interfere with the property;
- where the application is made under section 23, details of the authorisation for covert surveillance to which the application relates;
- in case of a renewal, the results obtained so far, or a full explanation of the failure to obtain any results; and
- whether an authorisation was granted or refused, by whom and the time and date on which this happened.

6.20. In urgent cases, the above information may be supplied orally. In such cases, the authorising officer and the applicant should also record the following information in writing, as soon as is reasonably practicable (it is not necessary to record further detail):

- the identity or identities of those owning or using the property (where known);
- sufficient information to identify the property which will be affected;
- details of the offence suspected or committed; and
- in urgent cases, the reasons why the authorising officer considered the case so urgent that an oral instead of a written authorisation was granted or, where an authorisation was granted in writing by an authorising officer whose entitlement to act is confined to urgent applications, the reasons why it was not reasonably practicable for the application to be considered by the authorising officer whose entitlement to act is not so confined.

Notifications to IPC

6.21. The IPC must be notified of all authorisations, renewals and cancellations for entry on or interference with property, in accordance with procedures under RIPO. In the case of non-urgent CI authorisations, prior approval of the IPC must be obtained before the authorisation comes into effect.

Duration of authorisations

6.22. Written authorisations for entry on or interference will cease to have effect at the end of a period of 3 months beginning with the day on which they took effect. So an authorisation granted at 09.00 on 12 February will expire on 11 May. (Authorisations (except those lasting for 72 hours) will cease at 23.59 on the last day.)

6.23. In the case of non-urgent CI authorisations, which require the prior approval of the IPC, the duration of an authorisation is calculated from the time at which the person who gave the authorisation was notified that the IPC had approved it. This can be done by presenting the authorising officer with the approval decision page to note in person or, if the authorising officer is unavailable, sending the written notice by auditable electronic means. In cases not requiring prior approval, the duration of an authorisation is calculated from the time the authorisation was granted.

6.24. Oral authorisations granted in urgent cases by authorising officers orally, and written authorisations granted by a person entitled to act only in urgent cases, will cease at the end of the period of 72 hours beginning with the time when they took effect.

Renewals

6.25. If at any time before the time and day on which an authorisation expires, the authorising officer considers the authorisation should continue to have effect for the purpose for which it was issued, he may renew it in writing for a period of 3 months beginning with the day on which the authorisation would otherwise have ceased to have effect. Authorisations may be renewed more than once, if necessary, and details of the renewal should be centrally recorded (see Chapter 7).

6.26. The IPC must be notified of renewals of authorisations for the entry on or interference with property. If, at the time of the renewal, the authorisation becomes a CI authorisation, the prior approval of the IPC must be sought before the renewal can take effect in a non-urgent case. The fact that the initial authorisation was a CI authorisation and therefore required the approval of the IPC before taking effect does not mean that its renewal will automatically require such approval. It will only do if, at the time of renewal, it is a CI authorisation (and not an urgent case).

Cancellations

6.27. The authorising officer who granted or last renewed the authorisation must cancel it if he is satisfied that the authorisation no longer meets the criteria upon which it was authorised. 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 the authorising officer.

6.28. Following the cancellation of the authorisation, the IPC must be notified of the cancellation.

6.29. The IPC may cancel an authorisation if satisfied that, if at any time after an authorisation was granted or renewed, there were no reasonable grounds for believing that it should subsist: see section 29(2) of RIPO. In such circumstances, the IPC may order the destruction of records, in whole or in part, other than any that are required for pending criminal or civil proceedings.

6.30. Once an authorisation or renewal is cancelled, the authorising officer must immediately give an instruction to cease all the actions authorised for the entry on or interference with property. The time and date when such an instruction was given should be centrally retrievable for at least 3 years (see Chapter 7).

Retrieval of surveillance equipment

6.31. Because of the time it can take to remove equipment from a person's property, it may also be necessary to renew an authorisation in order to complete the retrieval. The renewal should state why the operation is being or has been closed down, why it has not been possible to remove the equipment and, where possible, a timescale for removal.

7.0. Record keeping and error reporting

Centrally retrievable records of authorisations

Covert surveillance authorisations

7.1. A record of the following information pertaining to all authorisations must be centrally retrievable for a period of at least 3 years from the ending of each authorisation. This information should be regularly updated whenever an authorisation is granted, renewed or cancelled and should be made available for any relevant inspection upon request:

- the type of authorisation;
- the date the authorisation was granted;
- the name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- whether the urgency provisions were used, and if so why;
- if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation; and
- the date the authorisation was cancelled.

7.2. The following documentation should also be centrally retrievable for at least 3 years from the ending of each authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval granted by the authorising officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the authorising officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction to cease surveillance was given; and
- the date and time when any other instruction was given by the authorising officer.

Property interference authorisations

7.3. The following information relating to all authorisations for the entry on or interference with property should be centrally retrievable for at least 3 years:

- the time and date when an authorisation is granted;

- whether an authorisation is in written or oral form;
- the time and date when it was notified to the IPC;
- every occasion when entry on or interference with property has occurred;
- the result of periodic reviews of the authorisation;
- the date of every renewal; and
- the time and date when any instruction was given by the authorising officer to cease the interference with property

Retention of records

7.4. Records must be available for inspection by the Investigatory Powers Commissioner. Although records are only required to be retained for at least three years, it is desirable, if possible, to retain records for up to five years.

Errors

7.5. This section provides information regarding errors. Proper application of the surveillance 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 authorisations, reducing the scope for making errors.

7.6. 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.

7.7. 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 RIPO.

7.8. 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.

7.9. 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.

7.10. 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.

7.11. 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 surveillance or property interference 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.

7.12. 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 Commissioners.

7.13. In addition to the above, errors may arise where an 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 public 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 7.9 apply as they apply to the reporting of a relevant error.

Serious errors

7.14. 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 2004) is not sufficient by itself for an error to be a serious error.

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

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

7.16. 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. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

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

8.0 Safeguards

Use of material as evidence - general

8.1. Subject to the provisions of Chapter 4, material obtained through covert surveillance or the entry on or interference with property 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 that legislation, obtaining appropriate authorisations should help ensure the admissibility of evidence.

Retention and destruction of material.

8.2. Investigating authorities must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of covert surveillance or property interference.

8.3. Where the product of surveillance or property interference 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.

8.4. Subject to the provisions of Chapter 4, there is nothing in RIPO which prevents material obtained under covert surveillance or property interference authorisations from being used to further other investigations.

Reviewing authorisations

8.5. 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 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.

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

Handling material

8.7. Paragraphs 8.8 – 8.14 below provide guidance as to the safeguards which govern the dissemination, copying, storage and destruction of private information obtained through covert surveillance or property interference. Each investigating authority must ensure that there are internal arrangements in force for securing that the requirements of these safeguards are satisfied in relation to private information obtained by these means. Authorising officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the

Data Protection Ordinance 2020 and any relevant internal arrangements produced by individual authorities relating to the handling and storage of material.

Dissemination of information

8.8. Material acquired through covert surveillance or property interference will 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. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary for the authorised purpose(s) set out above. This obligation applies equally to disclosure to additional persons within an investigating authority and to disclosure outside the authority. 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.

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

8.10. Where material obtained under an authorisation is disclosed to the authorities of a country or territory outside the SBAs, the investigating authority must ensure that the material is only handed over to the authorities if it appears to them that any requirements relating to minimising the extent to which material is disclosed, copied, distributed and retained will be observed to the extent that the authorising officer considers appropriate.

Copying

8.11. Material obtained through covert surveillance or property interference may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Storage

8.12. Material obtained through covert surveillance or property interference, and all copies, extracts and summaries of it, 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.

8.13. 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

8.14. Information obtained through covert surveillance or property interference, 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(s). 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.

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 covert surveillance and entry on or interference with property;
- 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 relevant inspectors when they conduct their inspections; 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 or 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.