保安局檔號：ICSB 22/06

《截取通訊及監察條例草案》委員會

實務守則

本文件載述在條例草案成為法例後, 依據第 59 條而訂立的實務守則的最新版本擬稿。本擬稿以草案為基礎擬訂，並參考了當局的委員會階段修正案及法案委員會在審議草案時提出的建議。

2. 基於其性質，實務守則只能在條例草案成為法例後才能有最後定稿。例如守則中草案條文的編號須加以修訂。我們亦會繼續考慮執法機關從實際運作的角度提出的意見，而對守則擬稿作出修訂，例如，考慮使用常用的報告輔助工具如流程圖等，以助人員理解本守則的內容。因此，本守則仍然須作出一些修改。

3. 一如以往所指出，實務守則將刊登憲報，亦會提供給保安事務委員會省閱。

保安局
2006 年 7 月

註：實務守則擬稿請參閱本文件英文版本。

Interception of Communications and Surveillance Ordinance

Code of Practice

Pursuant to Section 59 of the Interception of Communications and Surveillance Ordinance

Note: Annex not attached.

GENERAL

This Code of Practice (this "Code") is issued under section 59 of the Interception of Communications and Surveillance Ordinance, Cap. XXX (the "Ordinance") to provide practical guidance to officers of the departments listed in Parts 1 and 2 of Schedule 1 to the Ordinance. Under the Ordinance, non-compliance with this Code constitutes non-compliance with the "relevant requirements" of the Ordinance[1], and has to be reported to the Commissioner on Interception of Communications and Surveillance (the Commissioner). Officers are reminded to comply with this Code at all times.

2. Any non-compliance with this Code and other relevant requirements should be brought to the attention of the management of the department without delay[2]. Depending on the circumstances of the case, the relevant officer may be subject to disciplinary action or the common law offence of misconduct in public office, in addition to the full range of existing law.

3. Unless the context otherwise requires, the interpretation of terms used in this Code should follow that set out in the Ordinance.

4. All officers are prohibited from carrying out any interception, either directly or indirectly (whether through any other person or otherwise), unless –

(a) the interception is carried out pursuant to a prescribed authorization under the Ordinance;

(b) the interception is of telecommunications transmitted by radiocommunications (other than mobile phones); or

---

1 "Relevant requirement" means any applicable requirement under any provision of the Ordinance, the code of practice or any prescribed authorization or device retrieval warrant concerned.

2 Please see paragraphs 7 and 148 to 149 below.

(c) the interception is authorized under other enactments[3].

5. Similarly, all officers are prohibited from carrying out any covert surveillance, either directly or indirectly (whether through any other person or otherwise), unless the surveillance is carried out pursuant to a prescribed authorization under the Ordinance.

6. This Code sets out further practical guidance for prescribed authorizations in respect of interception and covert surveillance under paragraphs 4(a) and 5 respectively.

7. Officers are also reminded to observe the requirements of the prescribed authorization fully in carrying out operations under the Ordinance, and nothing should be done in excess of what is authorized. Should any officer discover that any interception or covert surveillance is being or has been carried out without the authority of a prescribed authorization, it should be stopped immediately, followed by a report to the management of the department as soon as reasonably practicable. The head of department should cause a report on any such irregularity to the Commissioner to be made.

INTERCEPTION OF COMMUNICATIONS

8. The interpretation of the relevant terms such as "postal interception", "telecommunications interception" and "intercepting act" is set out in section 2(1) of the Ordinance. As regards "data produced in association with the communication" in section 2(5) of the Ordinance, it includes such data as the telephone number of the caller and recipient, and other data that identify

---

[3] These include, for example, the examination of postal packets held in the custody of the Post Office empowered under section 35 of the Import and Export Ordinance, Cap. 60; the search, reading and stoppage of mail in respect of inmates empowered under Rules 47, 47A, 47B and 47C of the Prison Rules (Cap. 234, sub. leg. A); and the control over the communications of the inmates of mental hospitals with outsiders under the Mental Health Regulations (Cap. 136, sub. leg. A).

the source and recipient of communication (e.g. fax number or email address). The capture of such information without accessing the actual message of the communication during the course of transmission would still be regarded as interception. However, the obtaining of records, e.g. call records and telephone bills, after the communication has been transmitted, is not an intercepting act. Records of this type of information may be obtained by search warrants.

COVERT SURVEILLANCE

9. The interpretation of relevant terms such as "covert surveillance" and "surveillance device" is set out in section 2(1) of the Ordinance. Some related concepts are elaborated below.

10. The term "private information" should be given a broad interpretation, covering any information about a person's private and family life, including his personal relationship with others.

11. The test for determining whether a person is entitled to a "reasonable expectation of privacy" has two prongs. The first one is whether the person's conduct will exhibit a subjective expectation of privacy. The second is whether the person's subjective expectation of privacy is one that society is willing to recognize as reasonable[4]. The following factors may be relevant in assessing whether an individual's privacy expectation is reasonable –

(a) the place where the intrusion occurs (e.g., whether or not the place is open to public view);

(b) the object and occasion of the intrusion (e.g., whether it interferes with the private life of the individual);

---

[4] Hong Kong Law Reform Commission (LRC) *Report on Civil Liability for Invasion of Privacy* (2004), para. 6.26

(c) the means of intrusion employed and the nature of any device used; and

(d) the conduct of the individual prior to or at the time of the intrusion (e.g., whether the individual has taken any steps to protect his privacy)[5].

When in doubt, officers should seek legal advice as to whether a person is entitled to a "reasonable expectation of privacy" in the particular circumstances in question.

12. Under section 2(2) of the Ordinance, in relation to any activity carried out by a person in a public place, a person is not regarded as being entitled to a reasonable expectation of privacy. However, this does not affect any reasonable expectation of privacy that he may have in relation to words spoken, written or read by him in a public place. In other words, a person writing a letter in a public place may still be entitled to a reasonable expectation of privacy in respect of the content of the letter.

13. The term "public place" has the same meaning as that in section 2(1) of the Summary Offences Ordinance (Cap. 228), but does not include any such premises that are intended for use by members of the public as a lavatory or as a place for taking a bath or changing clothes. According to section 2(1) of Cap. 228, *"public place includes all piers, thoroughfares, streets, roads, lanes, alleys, courts, squares, archways, waterways, passages, paths, ways and places to which the public have access either continuously or periodically, whether the same are the property of the Government or of private persons."* Section 2(2) of Cap. 228 further provides that *"(w)here no specific description is given of the ownership of any property, the word 'property' shall be taken to*

---

[5] For more details, see LRC Report *Privacy : The Regulation of Covert Surveillance* (2006), para. 2.43.

apply to all such property of the kinds specified, whether owned by the Government, by a public department or by a private person." Premises include any conveyance under the Ordinance and hence "public place" also includes a means of transport made available to the public.

14. The Ordinance specifies two types of covert surveillance – "Type 1 surveillance" and "Type 2 surveillance". The interpretation of the two terms is set out in section 2(1) of the Ordinance.

15. The distinction between Type 1 and Type 2 covert surveillance reflects the different degrees of intrusiveness into the privacy of those who are subject to the surveillance. Type 2 surveillance covers "participant monitoring" situations where the words or activities of the target of surveillance are being listened to, monitored by or recorded by someone (using a listening device or optical surveillance device) whom the target reasonably expects to be so listening or observing. It also covers situations where the use of optical or tracking devices does not involve entry onto premises without permission or interference with the interior of conveyance or object, or electronic interference with the device, without permission. Any covert surveillance other than Type 2 surveillance is Type 1 surveillance.

16. Any covert surveillance which is otherwise Type 2 surveillance is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege (LPP) will be obtained by carrying it out.

17. "Permission" for the entry onto any premises means permission, either implied or express, and either general or specific, granted by the lawful owner or occupant of the premises, as appropriate, whether with conditions or not. No permission for entry is required where the premises are public places to which members of the public have access. Permission for the interference with a conveyance or object means permission, either implied or express, and

either general or specific, given by the lawful owner or the person having the right to exclusive use of the conveyance or object. A permission for entry obtained by deception is not regarded as permission.

18. As regards "surveillance device", apart from the four classes of device set out in the Ordinance, the Ordinance provides that further classes of device may be prescribed by regulation made under section 62 of the Ordinance.

PRESCRIBED AUTHORIZATIONS

19. A prescribed authorization under Part 3 of the Ordinance will provide lawful authority for departments specified in Schedule 1 to the Ordinance to carry out interception of communications or covert surveillance.

Relevant Authority

20. The relevant authority for authorizing prescribed authorizations will vary, depending on whether the prescribed authorization is for interception of communications, Type 1 surveillance or Type 2 surveillance, and whether the authorization applied for is an emergency authorization or not. The "relevant authority" for considering applications for prescribed authorizations is as follows –

(a) <u>Interception and Type 1 Surveillance</u>

- any panel judge.

(b) <u>Type 2 Surveillance</u>

- the authorizing officer designated by the respective head of the departments listed in Part 2 of Schedule 1 to the Ordinance. For the purpose, notwithstanding the minimum

rank (senior superintendent of police or equivalent) set out in the Ordinance, only officers at or above the following ranks may be so designated –

(i) in relation to the Customs and Excise Department, a member of the Customs and Excise Service at or above the rank of Chief Superintendent;

(ii) in relation to the Hong Kong Police Force, a police officer at or above the rank of Chief Superintendent;

(iii) in relation to the Immigration Department, a member of the Immigration Service at or above the rank of Senior Principal Immigration Officer ; or

(iv) in relation to the Independent Commission Against Corruption, an officer of its Operations Department at or above the rank of Principal Investigator.

(c) Emergency Authorization

- the head of a department[6].

21. For executive authorizations, in no case should –

(a) the authorizing officer be directly involved in the investigation of the case covered by the application for authorization;

(b) the applying officer be the same person as the authorizing officer; or

(c) the authorizing officer be involved in formulating the

[6] For the purpose of the Ordinance, the head of department includes the deputy head of department.

application.

Conditions for Issue, Renewal or Continuance of Prescribed Authorization

22. Section 3 of the Ordinance sets out the conditions for the issue or renewal, or the continuance, of a prescribed authorization for interception of communications or covert surveillance.

23. Section 2(1) defines the term "serious crime". The serious crime threshold is no more than an initial screen. Officers must be satisfied that the conditions in section 3 are met in the circumstances of the case regarding the particular serious crime before submitting an application.

24. An assessment of the impact of a particular threat to public security should include an assessment of the impact, both direct and indirect, of the threat to the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong. Advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely to be carried on by violent means, is ***not*** of itself regarded as a threat to public security.

25. As regards the other relevant matters that may be taken into consideration under section 3(1)(b)(iii), they include the rights and freedoms guaranteed by Chapter III of the Basic Law (such as freedom of speech and of the press, freedom of assembly, of procession and of demonstration, the right to confidential legal advice, the right to protection against intrusion into a person's home or other premises, and the freedom and privacy of communications).

26. As interception or covert surveillance may interfere with the privacy of persons other than the subject, it is necessary for the officer making the application to carry out a risk assessment of collateral intrusion and consider ways of minimizing such interference. Officers involved in the application and determination of prescribed authorizations should pay particular attention to

this concern when considering whether the necessity and proportionality tests in section 3 of the Ordinance would be met.

APPLICATION PROCEDURES

General Rules

27. The applicant for all applications made under the Ordinance should not be lower in rank than inspector of police or equivalent, and should be conversant with the facts of the case.

28. Apart from the information required to be provided under the Ordinance, if there is any other information that the applicants consider to be likely to affect the determination, it should be included in the affidavit / affirmation or statement in writing (as the case may be) as well. Where the particulars of previous applications are required to be provided, the determinations made in respect of such applications should also be included. The information provided should be sufficiently detailed to facilitate consideration on the basis of the written submission alone, if the relevant authority so decides. All applications except oral applications should be made in writing, and should be signed by the applicant. In this connection, officers are reminded that wilfully making a false affidavit, affirmation or statement is a criminal offence.

29. If a previous application relating to the same operation has already been refused, an officer must not submit the same application with materially the same details.

30. In assessing the duration of authorization or renewal to apply for, officers should carefully consider the circumstances of the case, and specify a period which is reasonable and justifiable. The term “period” may refer to either a specified time duration, or the occurrence of a specified event.

31. In exercising the powers under prescribed authorizations, officers shall maintain proper records to account for their actions.

32. To enable the relevant authority to consider applications in context, the supporting affidavit / affirmation or statement in writing must specify clearly what types of interception or covert surveillance are involved. As far as possible, specific details should be provided. For example, in the case of interception, the application should specify whether it is proposed to undertake postal interception or telecommunications interception and, in the latter case, whether the interception is of telephone conversations, emails, fax transmissions, etc. In the case of covert surveillance, the application should indicate the types of surveillance device (optical surveillance, listening, etc.) proposed to be used. The identifying details of the communications or activities to be intercepted or put under surveillance should also be provided as far as they are known to the applicant. These details include, for example, the address of the subject of postal interception, the telephone number of the subject of the line to be intercepted and the location at which the surveillance device will be used.

33. For the same investigation or operation, a single application may cover more than one subject. This is possible if the need to make an application on the same investigation or operation covering the various subjects arises at the same time. However, separate applications may also be made at different times for the same case during its investigation or operation to take into account developments, for example, the identification of another suspect. A separate application should be made for different investigations or operations.

Issue of Judge's Authorizations

34. This section applies to applications for the issue or renewal of a prescribed authorization for carrying out interception of communications or Type 1 surveillance, in accordance with Division 2 of Part 3 of the Ordinance.

The relevant authority for granting authorization for such applications is the panel judge.

Application for Judge's Authorization for Interception or Type 1 Surveillance

35. Upon obtaining an approval from a directorate officer of the department concerned, an officer of the department may apply to a panel judge for the issue of a judge's authorization for interception or Type 1 surveillance. The application shall be made in writing as per the format at **COP-1** at **Annex**.

36. The application shall be supported by an affidavit / affirmation of the applicant detailing the facts which are relied upon to obtain the judge's authorization. The affidavit / affirmation must contain the relevant information set out respectively in Parts 1 or 2 of Schedule 3 to the Ordinance (as the case may be). The affidavit / affirmation should be sworn / affirmed. This should as far as possible be done before one of the assistants to the panel judges, or the panel judges themselves, in order to protect the confidentiality of the information involved.

Determination of Application for Judge's Authorization by the Panel Judge

37. The panel judge will deliver in writing his determination[7], and will return the determination and the certified copy of the application, the affidavit / affirmation and other supporting documents submitted with the application to the applicant.

Duration of Judge's Authorization

38. Section 10 of the Ordinance provides for the duration of a judge's authorization. Paragraph 30 above is relevant.

---

[7] The panel judge may consider the application in such manner as he considers appropriate. Where the panel judge decides to hold a hearing in respect of the application, it will be held in private and the panel judge may arrange for the hearing to be audio-taped.

Renewal of Judge's Authorizations

39. If a judge's authorization in force has to be renewed, a renewal application must be made before the authorization ceases to have effect. A judge's authorization may be renewed more than once.

Application for Renewal of Judge's Authorization

40. Upon obtaining an approval from a directorate officer of the department, an officer of the department concerned may apply to a panel judge for renewal of the authorization. The application shall be made in writing as per the format at **COP-2** at **Annex**, and shall be supported by the documents set out in section 11(2) of the Ordinance (including a copy of the judge's authorization sought to be renewed, copies of all affidavits / affirmations provided for the purposes of any previous applications in relation to the issue or renewal of the judge's authorization, as well as an affidavit / affirmation of the applicant containing the information set out in Part 4 of Schedule 3 to the Ordinance).

41. Other detailed arrangements in respect of the affidavit / affirmation as set out in paragraph 36 above apply. Any renewal of the same authorization for more than five times should be reported to the Commissioner.

Determination of Renewal of Judge's Authorization

42. The panel judge will deliver in writing his determination, and will return the determination and the certified copy of the application, the affidavit / affirmation and other supporting documents submitted with the application to the applicant.

Duration of Renewal of Judge's Authorization

43. Section 13 of the Ordinance provides for the duration of a renewal

of a judge's authorization. Paragraph 30 above is relevant.

Issue of Executive Authorizations

44. This section applies to applications for issue or renewal of a prescribed authorization for Type 2 surveillance in compliance with Division 3 of Part 3 of the Ordinance.

45. The relevant authority for considering such applications is the authorizing officer designated by the head of a department of a rank as stipulated in paragraph 20(b) above.

Applying for Type 1 authorization for Type 2 surveillance

46. Section 2(3A) of the Ordinance provides that an officer may apply for the issue or renewal of a Type 2 surveillance authorization as if the Type 2 surveillance were Type 1 surveillance, and the provisions of the Ordinance relating to the application and the prescribed authorization apply to the Type 2 surveillance as if it were Type 1 surveillance. Officers should consider making an application for Type 1 authorization if the operation would involve both Type 1 and Type 2 surveillance, thus obviating the need to apply for two separate authorizations for the same operation.

47. In addition, special circumstances of a Type 2 surveillance operation may render it particularly intrusive, e.g.,

- there is a likelihood that contents of journalistic material may be obtained; or

- an electronic optical surveillance device is proposed to be directed at a person inside premises from outside those premises in circumstances where the person has taken measures such that, were it not for the use of that device, he would not be observable by a person outside the

premises.

In such situations, consideration should be given to applying for a Type 1 authorization.

Application for Issue of Executive Authorization

48. An application for executive authorization shall be made in writing and supported by a statement in writing made by the applicant detailing the facts which are relied upon to obtain the executive authorization. The statement should contain the relevant information set out in Part 3 of Schedule 3 to the Ordinance (**COP-8** and **COP-9** at **Annex**).

49. Should the case involve participant monitoring in Type 2 surveillance, the consent of the participating party should be obtained prior to the operation taking place, and this should be so indicated in making the application.

Determination of Application for Executive Authorization by the Authorizing Officer

50. The authorizing officer may seek additional information from the applying officer as he deems appropriate. In such case, he shall record the additional information in writing, if it is not provided in written form. After considering the application, the authorizing officer shall deliver in writing his determination (**COP-10** or **COP-11** at **Annex**).

51. In considering an application, an authorizing officer must be satisfied that the conditions for issuing the authorization set out in section 3 of the Ordinance (see paragraphs 22 to 26 above) are all met. The particular intrusiveness of the operation because of the nature of the information that may be obtained (such as journalistic material), the identity of the subject (such as

lawyers), etc. may be relevant (paragraph 47 above). In particular, special attention should be paid to the assessment of the likelihood of information that is subject to LPP may be obtained. If LPP information is likely to be obtained through the proposed operation, an application for Type 1 authorization from a panel judge should be made (paragraph 16 above).

Duration of Executive Authorization

52. Section 16 of the Ordinance provides for the duration of an executive authorization. Paragraph 30 above is relevant.

Renewal of Executive Authorization

53. If an executive authorization in force has to be renewed, a renewal application must be made before the executive authorization ceases to have effect. An executive authorization may be renewed more than once.

Application for Renewal of Executive Authorization

54. An officer of the department concerned may apply to an authorizing officer of the department for renewal of executive authorization. The application shall be made in writing as per the format at **COP-12** at **Annex**. The application is to be supported by the documents set out in section 17(2) of the Ordinance (including a copy of the executive authorization sought to be renewed, copies of all statements provided for the purposes of any previous applications in relation to the issue or renewal of the executive authorization, as well as a statement in writing by the applicant containing the information set out in Part 4 of Schedule 3 to the Ordinance, with the sample form at **COP-13** at **Annex**).

55. Other arrangements in respect of the statement as set out in paragraph 48 above apply. Any renewal of the same authorization for more

than five times should be reported to the Commissioner.

Determination of Application for Renewal of Executive Authorization

56. The authorizing officer shall deliver in writing his determination (**COP-14** or **COP-15** at **Annex**).

Duration of Renewal of Executive Authorization

57. Section 19 of the Ordinance provides for the duration of a renewal of an executive authorization. Paragraph 30 above is relevant.

Emergency Authorizations

58. This section applies to applications for emergency authorizations for the carrying out of interception of communications or Type 1 surveillance under Division 4 of Part 3 of the Ordinance. The head of the department (including the deputy head) is vested with the authority to issue emergency authorizations under specified circumstances.

Application for Emergency Authorization

59. Section 20 of the Ordinance provides that an officer of a department may apply to the head of the department for the issue of an emergency authorization for interception or Type 1 surveillance under the specified circumstances. It refers to, inter alia, the terms "imminent risk", "substantial damage" and "vital evidence". What constitutes such risk, damage or evidence depends much on the circumstances of each case. In general terms, an "imminent" risk is a very near and impending risk. For example, if there is reliable intelligence indicating that the event will take place within a matter of a few hours, it is imminent. "Substantial" damage is damage which is large in amount, or extent. "Vital" evidence is evidence which is necessary or very important in supporting a case. For example, the

destruction of a weapon used in a murder would constitute loss of vital evidence. The applying officer (and the endorsing officer, if applicable) should be satisfied that the gravity of the case justifies the emergency authorization.

60. Officers are reminded that an application for emergency authorization should only be made if it is not reasonably practicable in the circumstances to apply for a judge's authorization, even by oral application. It should only be used as a last resort. A judge's authorization should be applied for whenever it is reasonably practicable to do so.

61. The application for emergency authorization shall be in writing and supported by a statement in writing made by the applicant (**COP-22** or **COP-23** at **Annex**) detailing the facts which are relied upon to obtain the emergency authorization. The statement must contain the information set out in Parts 1 or 2 of Schedule 3 to the Ordinance (as the case may be) in respect of affidavit / affirmation required for judge's authorization.

Determination of Application for Emergency Authorization

62. The head of the department shall deliver in writing his determination (**COP-24** or **COP-25** at **Annex**). He shall not approve the emergency authorization unless he is satisfied with the emergency conditions (see paragraph 59) and the conditions for issuing the authorization set out in section 3 of the Ordinance (see paragraphs 22 to 26 above) are all met.

Duration of Emergency Authorization

63. Section 22 of the Ordinance provides for the duration of an emergency authorization. Paragraph 30 above is relevant. In addition, the exact time when the emergency authorization begins to have effect should be specified, i.e., it should include the date and hour.

Application for Confirmation of Emergency Authorization

64. The Ordinance provides that where any interception or Type 1 surveillance is carried out pursuant to an emergency authorization, the head of the department concerned shall cause an officer of the department to apply to a panel judge for confirmation of the emergency authorization, as soon as reasonably practicable after, and in any event within, the period of 48 hours beginning with the time when the emergency authorization takes effect, irrespective of whether the operation has been completed or not. Unless directed otherwise, the original applicant of the application should make the application for confirmation.

65. The application should be made in writing. And apart from a copy of the statement in writing made under section 20(2)(b) of the Ordinance for the purposes of the application for the issue of the emergency authorization (see paragraph 61 above), it should also be supported by the documents set out in section 23(2) of the Ordinance (including a copy of the emergency authorization, as well as an affidavit / affirmation of the applicant which is to verify the contents of the above-mentioned statement for the purposes of the application for the issue of the emergency authorization).

66. It is essential that all application for confirmation of an authorization be made within 48 hours of the emergency authorization. Section 23(3) of the Ordinance provides that in default of any application being made for confirmation of the emergency authorization within the 48 hours, the head of the department concerned shall –

> *"(a) cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned; and*

(b) ……submit to the Commissioner a report with details of the case."

In this connection, "information" includes all products as well as any other information obtained by carrying out the operation.

67. To ensure compliance with the requirement to apply for confirmation within the 48-hour limit, heads of departments should put in place arrangements for emergency authorizations to be closely tracked, and that their personal attention be brought to any failure to comply with the requirement to apply for confirmation within 48 hours.

68. Any failure to apply for confirmation of an authorization is a grave irregularity and will be viewed most seriously. Apart from the destruction of information obtained by carrying out the operation (including products and any other information derived therefrom), the head of the department concerned shall cause a report to be made to the Commissioner without delay on the irregularity, with an explanation of the remedial action taken or to be taken to deal with the case in question and to prevent recurrence. The Commissioner is required under the Ordinance to conduct a review on the case. He may give notice to the target of the operation if the operation has been carried out without authority.

Determination of Application for Confirmation of Emergency Authorization

69. Under the Ordinance, the panel judge will not confirm the emergency authorization unless he is satisfied that section 21(2)(b) of the Ordinance has been complied with in the issue of the emergency authorization. The panel judge will deliver his determination in writing.

70. Where the panel judge refuses to confirm the emergency authorization in its totality, he may make one or more of the orders set out under

section 24(3) of the Ordinance. The relevant head of department shall ensure that the necessary arrangements are in place to implement the order(s) made. In this connection, "information" has the same meaning as set out in paragraph 66.

71. Where the emergency authorization is revoked, it shall cease to have effect from the time of the revocation. An emergency authorization may not be renewed. If necessary, an application to continue the interception or Type 1 surveillance in question may be made at the same time when making the application for confirmation of an emergency authorization.

Oral Applications

72. This section applies to oral applications for the issue of a judge's authorization, an executive authorization or an emergency authorization, and for renewal of judge's authorization and executive authorization, under Division 5 of Part 3 of the Ordinance[8].

Oral Application for Prescribed Authorizations

73. An application for the issue or renewal of a prescribed authorization provided under the Ordinance may be made orally, if the applicant considers that it is not reasonably practicable, having regard to all the circumstances of the case, to make the application in accordance with the relevant written application provisions, but it is still practicable to submit the application to the same relevant authority as for a written application. For example, in an urgent case involving serious bodily harm, although it is not possible to have the supporting affidavit / affirmation in writing to be prepared, it may still be practicable for an applicant to appear before a panel judge to

[8] As oral application is not available to device retrieval warrants, this section does not apply to applications for such warrants. Application for confirmation of emergency authorizations may not be made orally either.

apply for an authorization to carry out interception. Another example is where the written statement may have been prepared, the applicant cannot appear before the authorizing officer in person but may only contact him by telephone due to, say, very adverse weather conditions or bad road conditions. Also, if arrangements have to be made for the applicant to take part in a participant monitoring Type 2 surveillance operation that will take place very soon, an oral application may be made.

74. The oral application procedures under the Ordinance cater for special circumstances where the normal written application procedures cannot be followed. They should only be resorted to in exceptional circumstances.

75. Where an oral application is made, the information required to be provided for the purposes of the application may be provided orally and accordingly any requirement as to the making of any affidavit / affirmation or statement in writing does not apply. For the purpose of the Ordinance, *"an application is regarded as being made orally……[, and] information is regarded as being provided orally, if it is made orally in person or made by telephone, video conferencing or other electronic means by which words can be heard (whether or not any part of the application is made in writing)"*.

76. Where an oral application is made, the relevant authority may deliver orally his determination and, where applicable, give the reason for the determination orally.

77. Panel judges will audio-record the proceedings of oral applications made to them, or, in cases where recording is not practicable, make a written record of the applications. For executive authorizations and emergency authorizations, the authorizing officer should make a written record of the oral application and his determination with sufficient details to enable checking against the confirmation application.

Application for Confirmation of Prescribed Authorization or Renewal Issued or Granted upon Oral Application

78. The Ordinance provides that where, as a result of an oral application, the prescribed authorization or renewal sought under the application has been issued or granted, the head of the department concerned shall cause an officer of the department to apply to the same relevant authority for confirmation of the prescribed authorization or renewal, as soon as reasonably practicable after, and in any event, within the period of 48 hours beginning with the time when the prescribed authorization or renewal takes effect. Unless directed otherwise, the original applicant of the oral application should make the application for confirmation.

79. The application should be made in writing and should be supported by the documents set out in section 26(2) of the Ordinance. Apart from a record in writing containing all the information that should have been provided to the relevant authority in writing under the application form, it should also include an affidavit / affirmation or statement in writing (as the case may be) which is to verify all information provided orally during the initial oral application, as well as a record in writing setting out the determination delivered orally in respect of the initial oral application.

80. The application documents for judge's authorization, executive authorization and emergency authorization are set out respectively at **COP-4, COP-5, COP-16 to COP-18, COP-26 and COP-27** at **Annex**. It is essential that an application for confirmation be made within 48 hours. Otherwise, similar considerations as in paragraphs 66 to 68 above apply.

Determination of Application for Confirmation of Oral Application

81. After considering an application for confirmation of an executive

authorization or its renewal, the authorizing officer should deliver in writing his determination (**COP-19** or **COP-20** at **Annex**).

82. The Ordinance provides that the relevant authority shall not confirm the prescribed authorization or renewal unless he is satisfied that the relevant conditions provisions of the Ordinance have been complied with in the issue or granting of the prescribed authorization or renewal (see paragraphs 22 to 26 above).

83. When the relevant authority refuses to confirm the prescribed authorization or renewal in its totality, he may make one or more of the orders set out in section 27(3) of the Ordinance. The head of department shall ensure that the necessary arrangements are in place to implement the order(s) made. In this connection, "information" has the same meaning as set out in paragraph 66.

84. Where the prescribed authorization or renewal is revoked, the prescribed authorization or renewal shall cease to have effect from the time of the revocation.

Special Case of Emergency Authorization Issued as a result of Oral Application

85. For confirmation of an oral application for an emergency authorization, the head of the department concerned shall deliver his determination for the application for confirmation of an oral application in respect of an emergency authorization (**COP-28** or **COP-29** at **Annex)**. This would then need to be followed by a separate application to a panel judge for confirmation of the emergency authorization in accordance with the procedures set out in paragraphs 64 to 71.

86. To obviate the need for two separate applications to be made as described above, section 28 of the Ordinance sets out special arrangements

regarding the confirmation of an oral application for an emergency authorization directly to a panel judge. This procedure should be followed in normal circumstances, i.e. only one application for confirmation from the panel judge should be made. The applicant should prepare an application as per the format at **COP-4** at **Annex** and an affidavit / affirmation. The application should be made in writing and supported by the documents set out in section 28(2) of the Ordinance (broadly similar to those set out in paragraph 79 above). Other arrangements regarding the application and determination of application for confirmation of emergency application as set out in paragraphs 64 to 71 are applicable.

Implementation Aspects

What a prescribed authorization authorizes

87. A prescribed authorization for interception may be address-based (section 29(1)(a)(i) of the Ordinance), service-based (section 29(1)(b)(i)) or subject-based (section 29(1)(a)(ii) and (b)(ii)).

88. A subject-based authorization for interception allows the interception of telecommunications made to or from any telecommunications service that the subject is using, or is likely to use, or the interception of postal communications made to or by him, as the case may be. In the case of telecommunications interception, this caters for situations where the telecommunications service that the subject is using or is likely to use is either not known at the time of the application for the authorization or is likely to change during the course of the operation. In the case of postal interception, this caters for situations where the postal address of the subject is either not known at the time of the application for the authorization or is likely to change during the course of the operation.

89. An applicant should make the best endeavors to first establish the telecommunications service or postal address that are known to be used by the subject and apply for a service-based or address-based authorization as far as possible. If need be, a subject-based cum service- or address-based authorization may be applied for. An application for a subject-based authorization should only be made with strong justifications where other means of investigation, including service-based interception authorization, have been tried and have failed or have been considered and are either not available or are not suitable in the circumstances of a particular case. The applicant must state in the application why he believes that the subject will likely change the telecommunications service or postal address frequently.

90. For subject-based authorizations for interception, the inclusion of any new telephone number, email address, postal address etc. that the subject is using or is likely to use for carrying out the authorized interception operations may only be done with the approval of an officer not below the rank equivalent to that of a senior assistant commissioner of police, and only when there is reasonable ground to believe that the subject is using or is likely to use the telephone number, email address, postal address etc. The requirement "is using or likely to use" means that it would be inappropriate to include a telecommunications service or postal address the subject may only use incidentally. The reason for including the telecommunications service or postal address on the list should also be documented and submitted with the application for approval by the senior departmental officer for inclusion. The head of department should ensure that arrangements are made to keep a proper record on the identifying details of the communications intercepted for a subject-based authorization.

91. Similarly, it is incumbent on the same responsible officer to keep under review the list of included telecommunication service etc., with a view to

deleting from the list any telecommunication service or address etc. that the subject is no longer using or is unlikely to use. Again the deletion and the reason should be properly recorded.

92. A prescribed authorization for covert surveillance may be premises-based (section 29(2)(a) of the Ordinance), object-based (section 29(2)(b)) or subject-based (section 29(2)(c)).

93. A subject-based authorization for covert surveillance caters for situations if the subject has to be kept under surveillance for a continuous period and the place(s) where he is or is likely to be are likely to change or it is not known at the time of application for authorization where the subject is or is likely to be.

94. For subject-based authorizations for covert surveillance, Type 1 surveillance may only be carried out on premises when there is reasonable ground to believe that the subject is or is likely to be on the premises. The head of department should ensure that arrangements are made to keep a proper record on the premises on which Type 1 surveillance is carried out under a subject-based authorization.

95. A prescribed authorization, other than an executive authorization, may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized or required to be carried out under the prescribed authorization. And if it is necessary for the execution of the prescribed authorization, it may also contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned). An applicant should set out as clearly as possible the concealment or interference with property sought to be authorized.

96. A prescribed authorization, other than an executive authorization, may contain terms that require any person specified in the prescribed authorization (whether by name or by description) to provide to any of the officers of the department concerned such assistance in the execution of the prescribed authorization as is specified in the prescribed authorization. The person from whom such assistance is sought should be given reasonably sufficient time and explanation to understand the assistance that he has to provide, and be given a detailed explanation in case he has any doubt on being shown a copy of the prescribed authorization. It is important to obtain the assistance through cooperation and understanding to protect the confidentiality of the operation.

97. Sections 29(6) and (7), and 30 cover other matters which are essentially incidental to the authorization. Nonetheless, officers are reminded that any such conduct is only permissible to the extent that it is necessary for the execution of a prescribed authorization. Undertaking any conduct that is more than necessary for the execution of the authorization would not be covered by the authorization, and the acts concerned may not be immune from civil or criminal liabilities.

Protection of LPP information

98. As with all other law enforcement actions, departments shall in no case knowingly seek to obtain information subject to LPP in undertaking covert operations authorized under the Ordinance. Indeed, the Ordinance seeks to minimize the chance of inadvertently obtaining information subject to LPP during such operations. Section 30A prohibits the carrying out of interception or covert surveillance in a lawyer's office, residence and other relevant premises in the circumstances described in that section unless exceptional circumstances exist. Examples of relevant premises include interview rooms of courts,

prisons, police stations and other places of detention where lawyers regularly provide legal advice to their clients.

99. Officers should therefore take extreme care when approaching possible applications that concern the premises and/or telecommunications services used by a lawyer. A risk assessment must be conducted if the interception or covert surveillance may acquire information subject to LPP. In this connection, officers are reminded that LPP is not lost if a lawyer is properly advising a person who is suspected of having committed a criminal offence. Unless they are fully satisfied that the exceptional circumstances under section 30A of the Ordinance exist, officers should not make an application for an authorization targeting these premises and telecommunications services. In all such exceptional cases, a judge's authorization must be obtained even if the operation sought to be carried out would otherwise be a Type 2 surveillance operation under normal circumstances.

100. Any information that is subject to LPP is to remain privileged notwithstanding that it has been inadvertently obtained pursuant to a prescribed authorization. Dedicated units separate from the investigation team shall screen out information protected by LPP, and to withhold such information from the investigators. The only possible exception to this arrangement is in operations involving participant monitoring where, for the safety of the participants participating in the conversation (including the victims of crimes under investigation, informants or undercover officers), or in situations that may call for the taking of immediate arrest action, there may be a need for the investigators to listen to the conversations in real time. In such circumstances, it will be specified in the application to the panel judge, who will take this into account in deciding whether to issue an authorization and, if so, whether any conditions should be imposed. After such an operation, investigators monitoring the operations will be required to hand over the recording to the

dedicated units, who will screen out any information subject to LPP before passing it to the investigators for their retention.

101. Where, further to the issue or renewal of a prescribed authorization, the officer designated for the purpose of section 55(2) of the Ordinance for the operation concerned becomes aware that the subject of the operation has been arrested, he should assess the effect of the arrest on the likelihood that any information which may be subject to LPP will be obtained by continuing the operation and report to the relevant authority.

102. On receiving the report, the relevant authority should revoke the prescribed authorization if he considers that the conditions for the continuation of the prescribed authorization are no longer met.

103. Any information subject to LPP should be destroyed and no records of it should be kept in any form. In the case of a prescribed authorization for a postal interception or covert surveillance, not later than 1 year after its retention is not necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted, and in the case of a prescribed authorization for a telecommunications interception, as soon as reasonably practicable. In no case should any such LPP information be used for any other purposes. (See also paragraph 140 below.)

104. In the case of postal interception or covert surveillance, if the defendant enjoying the privilege wants the record of the communication to be used as evidence, he can waive his privilege and ask the prosecutor to produce it. In the case when the client is not a defendant in the court proceedings, or is one of several defendants, if those defendants who do not enjoy the benefit of the privilege seek access to the LPP material, the prosecutor must refuse disclosure of this part of the covert surveillance or postal interception product to them should the client not waive his privilege.

105. Where there is any doubt as to whether any information subject to LPP has been obtained or about the handling or dissemination of information consisting of matters subject to legal privilege, legal advice should be sought.

Care in implementation

106. The safety of any device to be used, including the possible hazardous effects to health, should be carefully assessed before deployment. Any surveillance device with harmful effects on the health of either officers or the subjects of surveillance should not be used. And should any condition be set by a health authority for the use of a surveillance device, it should be drawn to the attention of officers. In no case should surveillance devices be implanted in, or administered to, a person without his prior consent.

107. Officers are reminded that a prescribed authorization may be issued or renewed subject to conditions. Where any conditions are imposed, officers must take care to ensure that they are observed in executing the authorization. Officers must also act within the terms of the authorization, and should not interfere with other items unnecessarily. For example, in the case of a postal interception, the authorization would only cover the examination of the packet. Insertion of any objects into the postal packet concerned is not allowed. See also paragraph 7.

108. There should be suitable control mechanisms in respect of operations under the Ordinance to guard against possible abuse of procedures. For example, in the case of postal interception, the examination should be carried out either in the presence of another party (such as postal officers), or by at least two officers of the department, one being a supervisory staff at the rank of Inspector or above. Officers should ensure that a report to record details of the examination is completed and duly signed by officers carrying out the examination. Such report should be made available for inspection by the

Commissioner.

109. Officers in charge of the operation should also take extra care in planning operations that involve sensitive premises or situations, such as bathrooms or toilets where a higher level of privacy may be expected, and tailor their operations accordingly.

110. Reasonable force should only be used if it is necessary for carrying out a prescribed authorization and should be kept to the minimum required.

111. The same minimization principle applies to any interference with property. While a prescribed authorization may authorize the interference with property, this is only to the extent incidental to and necessary for the implementation of the authorization. Officers should at all times ensure that such interference and any damage that might be caused to property is kept to the absolute minimum. In the event that any unavoidable damage is caused to property, all efforts must be made to make good the damage. This is necessary to minimize interference with property right, and is also essential for preserving the covertness of the operations. In any case of damage, a report should be made to the Commissioner on the remedial action that has been taken to make good the damage and, if the damage cannot be made good, the reasons. Explanation should also be provided if no compensation is offered under the latter situation. The Commissioner may make a report to CE under section 48 of the Ordinance or make a recommendation to the department concerned under section 50 of the Ordinance in respect of such cases. Where claims for damages from parties whose property has been interfered with in carrying out a prescribed authorization are received by the department concerned, they should be handled in the same manner as other cases arising from any law enforcement operations.

Device Retrieval Warrant

112. As a matter of policy, surveillance devices should not be left in the target premises after their use, in order to protect the privacy of the individuals affected and the covert nature of the operation. A prescribed authorization already authorizes the retrieval of a surveillance device within the period of authorization, and surveillance devices should be retrieved during the period of authorization. However, it is accepted that in some cases it may not be reasonably practicable to retrieve the device before the end of the authorization. Retrieval of the device may not be practicable, for example, where an object to which a device is attached has been taken out of Hong Kong. As a general rule, after the expiry of the authorization, unless it is not reasonably practicable to retrieve the device, an application must be made for a device retrieval warrant if the device has not been retrieved. In all cases, at the expiration of the authorization, the officer-in-charge of the operation should take all reasonably practicable steps as soon as possible to deactivate the device or to withdraw any equipment that is capable of receiving signals or data that may still be transmitted by a device if it cannot be deactivated.

113. Any decision of not applying for a device retrieval warrant where the device has not been retrieved after the expiry of an authorization should be endorsed by an officer at the directorate rank and a report on the decision, together with the reasons and steps taken to minimize possible intrusion into privacy by the device, should be submitted to the Commissioner. The Commissioner may then carry out a review based on the information provided and reasons advanced.

General Rules

114. The general rules on the application for issue and renewal of authorizations as set out paragraphs 27 to 32 are applicable to the application

for device retrieval warrant.

Application for Device Retrieval Warrant

115. Section 32 of the Ordinance applies to the application for device retrieval warrants.

116. The application shall be made in writing (**COP-6** at **Annex**). The application shall be supported by a copy of the prescribed authorization, and an affidavit / affirmation containing information specified in Schedule 4 to the Ordinance, in particular an assessment of the impact (if any) of the retrieval on any person and the need for the retrieval.

Duration of Device Retrieval Warrant

117. Section 34 of the Ordinance provides for the duration of a device retrieval warrant. Paragraph 30 above is relevant.

General Provisions of Device Retrieval Warrant

118. Sections 35 and 36 of the Ordinance set out what the warrant authorizes. If it is necessary to carry out any concealment or interference with property for retrieval, this should be specified in making the application so that it could be so authorized. While no specific authorization for other incidental conduct set out in section 36 of the Ordinance is required, officers are reminded that the conduct must be necessary for and incidental to carrying out the warrant. Otherwise the conduct would not be covered by the warrant. Officers are also reminded that a device retrieval warrant does not authorize the further use of the device and the enhancement equipment concerned.

SAFEGUARDS

INDEPENDENT OVERSIGHT AUTHORITY

Functions of the Commissioner

119. The Commissioner plays an important oversight role under the Ordinance. The functions of the Commissioner are to oversee the compliance by departments and their officers with the relevant requirements under the Ordinance. To enable the Commissioner to exercise his oversight, he is given the power to access any documents and require any person to answer any questions, for the purpose of carrying out his functions. Such documents or questions include those relating to the prescribed authorizations or the applications for the issue or renewal of prescribed authorizations. The Commissioner may also require any officer of the department to prepare a report on any case of interception or covert surveillance handled by the department. All officers are reminded of the critical importance of providing as much assistance to the Commissioner as possible, and of cooperating with him fully. Any failure to comply with the requests of the Commissioner under his power would be viewed most seriously, and the officer concerned will be liable to disciplinary actions.

Reviews by the Commissioner

120. The Commissioner may conduct reviews under a number of situations :

(a) review of any case or procedure of departments for the purpose of overseeing compliance with the relevant requirements;

(b) reviews of cases in respect of which a report has been

submitted to him concerning the failure to apply for confirmation of an emergency authorization or prescribed authorization or renewal issued or granted upon an oral application, or in general any failure to comply with any relevant requirement of the Ordinance;

(c) reviews of reports from LEAs relating to operations in which materials involving LPP have been obtained, damage to properties has been caused, or devices have not been retrieved after expiry of an authorization; and

(d) other reviews as he considers necessary on compliance by departments and their officers with the relevant requirements.

121. The Commissioner will notify the head of the department concerned of the findings of his reviews and may refer these findings to the Chief Executive, the Secretary for Justice or any panel judge or all of them.

122. On receiving the Commissioner's findings, the head of the department concerned should cause a report to be submitted to the Commissioner with details of any measures taken by the department to address any issues identified in the findings as soon as reasonably practicable, or within the period specified by the Commissioner. These measures include, inter alia, disciplinary actions and those at the various stages of the disciplinary process.

Examinations by the Commissioner

123. A person may apply to the Commissioner for an examination under section 42 of the Ordinance.

124. The Commissioner will conduct an examination applying the

principles applicable by a court on an application for judicial review to determine whether the operation alleged has been carried out without the authority of a prescribed authorization. The term "without the authority of a prescribed authorization" covers a number of scenarios, e.g. -

(a) if there has been an operation for which the department should have applied for an authorization but has not in fact done so, i.e. there is no prescribed authorization at all;

(b) if there has been an authorization but it does not confer the proper authority for the operation, including where the operation is beyond the terms contained in the authorization, for example –

(i) the operation has been carried out on a person, telephone number or address not intended to be covered by the authorization; or

(ii) a higher level of authorization should have been applied for; or

(c) if there has been an authorization but it is invalid, for example,

(i) there has been material procedural impropriety in making the application; or

(ii) information that was available and that was likely to have affected the determination as to whether to issue the authorization was not provided to the authorizing authority.

125. It will be up to the Commissioner to decide how to go about his

examination. Officers are reminded to afford the maximum cooperation and assistance to the Commissioner to facilitate his examination. Any failure of a department or its officer to comply with the requirement made by the Commissioner may be reported to the Chief Executive.

126. As required by the Ordinance, the Commissioner would not carry out or proceed with an examination and make any determination further to the examination if any relevant criminal proceedings are pending or are likely to be instituted, until the proceedings have been finally determined or disposed of, and, in case of criminal proceedings likely to be instituted, until they are no longer likely to be instituted. Arrangements should be in place to ensure that the Commissioner is informed of any of the above situations, when it comes to the knowledge of a department that the Commissioner is examining a case.

127. Should the Commissioner find a case in the applicant's favour, he would notify the applicant as long as doing so would not be prejudicial to the prevention or detection of crime or the protection of public security. Departments must bring to the Commissioner's attention all relevant factors to facilitate his making of a decision in this regard. On being informed of the Commissioner's determination in favour of the applicant, the head of the department concerned must ensure that a report be made to the Commissioner detailing the reasons for the conduct without authority and what steps he has taken (including any disciplinary action in respect of any officer) in respect of the case in particular and to prevent future recurrence in general.

128. If the Commissioner determines that the interception or covert surveillance has been carried out without authority but decides not to give notification for the reason that the prevention or detection of crime or the protection of public security would be prejudiced, there would be a continuing duty upon him to review from time to time whether continued non-notification

is justified. To assist the Commissioner in this aspect, the head of the department concerned shall cause a regular report at least on a quarterly basis to be submitted to the Commissioner to facilitate his determination of whether continued non-notification is justified. The final decision of when to notify rests with the Commissioner.

Notification by the Commissioner

129. Under section 46A(1) of the Ordinance, if the Commissioner considers that there is any case in which any interception or covert surveillance has been carried out by an officer a department on a subject without the authority of a prescribed authorization, the Commissioner would give notice to the subject. Similar requirements and arrangements as for examinations by the Commissioner apply. Again, the decision as to whether to notify rests with the Commissioner.

REGULAR REVIEWS BY DEPARTMENTS

130. The head of the department shall make arrangements to keep under regular review, at least on a quarterly basis, the compliance by officers of the department with the relevant requirements under the Ordinance, i.e., the provisions of the Ordinance, this Code and the prescribed authorizations. The reviews may consist of audit checks of past and live cases as well as theme-based targeted reviews regarding, for example, the handling of applications, keeping of records, and reports to the Commissioner.

131. The head of department shall also designate a reviewing officer under section 54(2) of the Ordinance to keep under review the performance by the authorizing officers of any function under the Ordinance. The reviewing officer should be at least a rank higher than the officer for approving the making of applications for judge's authorization and the authorizing officer under the

Ordinance. In practice, therefore, the reviewing officer should be at the rank of assistant commissioner of police or equivalent or above. The reviewing officer should, as far as practicable, be an officer who is or was not directly involved in the investigation or operation in question.

DISCONTINUANCE OF INTERCEPTION OR COVERT SURVEILLANCE

132. If an officer conducting reviews under section 54(1) or section 54(2) of the Ordinance is of the opinion that the ground for discontinuance of a prescribed authorization exists, he shall as soon as reasonably practicable after forming the opinion, cause the interception or covert surveillance concerned to be discontinued. In practice, this would mean that the officer should inform the officer of the department concerned who is for the time being in charge of the interception or covert surveillance of his decision, and the latter should so comply.

133. An officer must be assigned to be in charge of a covert operation for the purpose of section 55(2). Arrangements should be in place to ensure that he is made aware of the relevant information and developments that may constitute the ground for discontinuance.

134. The officer for the purpose of section 55(2) of the Ordinance –

(a) should, as soon as reasonably practicable after he becomes aware that the ground for discontinuance of the prescribed authorization exists, cause the interception or covert surveillance to be discontinued; and

(b) may at any time cause the interception or covert surveillance to be discontinued.

135. Where any interception or covert surveillance has been

discontinued, the officer who has caused the discontinuance shall, as soon as reasonably practicable after the discontinuance, cause a report on the discontinuance and the ground for the discontinuance to be forwarded to the same relevant authority to whom an application under the Ordinance for the issue or renewal of the prescribed authorization concerned has last been made for revocation of the prescribed authorization concerned.

136. A ground for discontinuance of an operation under a prescribed authorization exists if the conditions for the continuance of the prescribed authorization under section 3 of the Ordinance are not met. In considering whether the conditions are not met, the officer concerned should take into account information that is available at the time of the review. Situations that may require discontinuance of operation could include, for example, the relevant purpose of the prescribed authorization has been achieved, the emergence of new information indicating that there is no further need for the operation, all the information sought has already been obtained etc. For instance, in a telecommunications interception or Type 1 surveillance operation, where the degree of intrusion into the privacy of persons unconnected with the investigation has reached a level beyond what was originally envisaged in the application for authorization, it could render the continuation of the operation disproportionate to the purpose sought and hence discontinuance is required.

137. For covert surveillance operations, a device retrieval warrant should also be applied for at the same time as the report on discontinuance where the device has not been retrieved, unless it is not reasonably practicable to retrieve the device (in which case a report would need to be submitted to the Commissioner (see paragraph 112 to 113). The officer-in-charge of the operation should, at the same time, take all reasonably practicable steps as soon as possible to deactivate the device or to withdraw any equipment that is capable of receiving signals or data that may still be transmitted by a device if it

cannot be deactivated.

138. The forms for reporting on the discontinuance of an operation under a prescribed authorization are set out respectively at **COP-7, COP-21** and **COP-30** at **Annex**.

SAFEGUARDS FOR PROTECTED PRODUCTS

139. Where any protected product[9] has been obtained pursuant to any prescribed authorization, the head of the department should make arrangements to ensure that the requirements in section 56 of the Ordinance are satisfied.

140. As pointed out in paragraph 103 above, where any protected product contains any information that is subject to LPP, the head of the department concerned should ensure that the protected product that contains such information –

(a) in the case of a prescribed authorization for a postal interception or covert surveillance, is destroyed not later than 1 year after its retention ceases to be necessary for civil or criminal proceedings before any court that are pending or are likely to be instituted; or

(b) in the case of a prescribed authorization for a telecommunications interception, is as soon as reasonably practicable destroyed.

141. Owing to the sensitive nature of interception or covert surveillance operations, any unauthorized disclosure of information on these operations may seriously infringe the privacy of the persons concerned as well as jeopardize the

[9] Copies of protect products are subject to the same protection requirements as those for the products themselves under the Ordinance. "Copy" is defined to include any copy, extract or summary of the contents.

specific investigation or operation. To protect privacy and ensure the integrity of classified operations, details of each operation should only be made known on a strict "need to know" basis.

142. Departments should, on the basis of their operation, set up system(s) to document the information obtained from operations authorized under the Ordinance, with restricted access to the different types of information depending on the confidentiality level, and proper paper trail on access, disclosure and reproduction.

143. The Ordinance provides that any relevant telecommunications interception product is not admissible in evidence in any proceedings before any court other than to prove that a relevant offence (e.g. under the Telecommunications Ordinance (Cap. 106) or Official Secrets Ordinance (Cap. 521)) has been committed.

144. Notwithstanding the general non-admissibility policy, section 58(4) of the Ordinance provides for disclosure of "*any information obtained pursuant to a relevant prescribed authorization and continuing to be available to the department concerned [that] might reasonably be considered capable of undermining the case for the prosecution against the defence or of assisting the case for the defence.*" To ensure that this is observed, departments should require officers concerned in the telecommunications interception operations to look out for and, where appropriate, report on such materials that may be exculpatory. In case of doubt, legal advice should be sought.

RETENTION OF RECORDS

145. Each department should maintain a central registry to keep the records associated with applications for prescribed authorizations and related matters.

146. The central registry plays an important role to ensure that a complete record is kept and to facilitate the work of the Commissioner and internal reviews. To protect the confidentiality of the information kept, it is essential that strict access control be implemented. The established requirements for physical security protection, access control and "need to know" principle should be complied with. Each head of department must also ensure that audit trails are kept for all instances of access.

147. Section 57 of the Ordinance sets out a number of record keeping requirements. These records should be kept by the central registry. Should the officer-in-charge of the registry suspect any irregularity in access requests, he should immediately report it to the management of the department.

ENSURING COMPLIANCE

148. Officers who fail to comply with the provisions of the Ordinance, the provisions of this Code or the terms and conditions of the authorization or device retrieval warrant concerned would be subject to disciplinary action or, depending on the case, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law. Each department should therefore ensure that officers who may be involved in the application for, or determination of and execution of matters covered by the Ordinance are fully briefed on the various requirements. Refresher briefings should be arranged as and when this Code is updated or after an important review by the Commissioner or the reviewing officer that may be of general reference value. All non-compliance, and the remedial measures, should be reported to the Commissioner.

149. Each department should appoint an officer to answer questions from the department's officers regarding compliance with this Code and, more generally, all the relevant requirements. Should there be suggestions from

departments as to how this Code may be revised to ensure better compliance, they should be brought to the attention of the Security Bureau.

150. This Code, and future revisions thereof, will be gazetted for general information.

* * * * *

Secretary for Security
August 2006