Legislative Council Panel on Security

Results of study of matters raised in the Annual Report 2011 to the Chief Executive by the Commissioner on Interception of Communications and Surveillance

PURPOSE

Pursuant to section 49 of the Interception of Communications and Surveillance Ordinance (the Ordinance), the Commissioner on Interception of Communications and Surveillance (the Commissioner) submitted his Annual Report 2011 (the Report) to the Chief Executive in June 2012. This note sets out the Administration's views on the matters raised in the Report.

BACKGROUND

2. Interception of communications and covert surveillance operations are critical to the capability of our law enforcement agencies (LEAs) in combating serious crimes and protecting public security. The Ordinance, enacted in August 2006, provides for a statutory regime for the conduct of interception of communications and covert surveillance by the LEAs. The Commissioner, appointed by the Chief Executive on the recommendation of the Chief Justice pursuant to section 39 of the Ordinance, is responsible for overseeing the compliance by the LEAs with the relevant requirements of the Ordinance.

3. The Report covers the period from 1 January 2011 to 31 December 2011 (the report period). The Chief Executive has caused a copy of the Report to be laid on the table of the Legislative Council on 28 November 2012.

4. The Security Bureau, in consultation with the LEAs concerned, has studied the matters raised in the Report.

GENERAL OBSERVATIONS

5. The Ordinance provides for a statutory framework for the conduct of interception of communications and covert surveillance that

aims to strike a balance between the need for prevention and detection of serious crimes and the protection of public security on the one hand and the need for safeguarding the privacy and other rights of individuals on the other. It provides for a stringent regime with checks and balance to ensure that the LEAs' covert operations are carried out in accordance with the requirements of the Ordinance.

6. During the report period, interception of communications and covert surveillance operations carried out by the LEAs were under the tight control of the statutory framework under the Ordinance. The LEAs, panel judges, and relevant parties provided the support and cooperation that the Commissioner needed to perform his oversight and review functions under the Ordinance. With regard to interception operations, the Commissioner made the observation that the LEAs had acted in a responsible manner and complied closely with the requirements and spirit of the Ordinance, in that whenever it was no longer necessary or proportional to continue with the prescribed authorization, or part of it, discontinuance would be undertaken as soon as possible. The panel judges had handled the applications carefully and applied a rather stringent control over the duration of authorizations. The Commissioner also observed that the panel judges continued to be very cautious in dealing with cases that might possibly involve information subject to legal professional privilege (LPP) being obtained by an LEA. When it was assessed that there was such likelihood and if they granted the authorization or allowed it to continue, they would impose additional conditions. The additional conditions were stringent and effective in safeguarding the important right of individuals to confidential legal advice.

THE COMMISSIONER'S FINDINGS

7. The Commissioner stated in Chapter 7 of the Report that he had received from the LEAs nine reports of non-compliance or irregularities under the Ordinance during the report period. Four of these nine reports involved non-compliance and were submitted by the LEAs under section 54 of the Ordinance.[1] The Commissioner also discussed in Chapter 7 of the Report two outstanding cases brought forward from the Annual Report 2010.

---

[1] Under section 54 of the Ordinance, where the head of an LEA considers that there may have been any case of failure by the LEA or any of its officers to comply with any relevant requirement of the Ordinance, he shall submit to the Commissioner a report with details of the case.

8. The Commissioner did not make any finding that any of the cases of non-compliance or irregularity was due to deliberate flouting or disregard of the statutory provisions or the law by the LEAs; nor did he find any of the officers committing the mistakes being actuated by ulterior motive or ill will. The incidents were mainly consequences of inadvertent or careless mistakes, or unfamiliarity on the part of certain officers with the rules and procedures of the ICSO scheme, which were uniquely related to the individuals concerned, rather than defects in any of the control systems. LEAs have taken follow up actions on these cases of non-compliance or irregularity in accordance with the Commissioner's advice and recommendations.

THE COMMISSIONER'S RECOMMENDATIONS TO THE ADMINISTRATION

9. Under section 40(b)(iv) of the Ordinance, without limiting the generality of the Commissioner's function of overseeing the compliance by the LEAs and their officers with the relevant requirements of the Ordinance, the Commissioner may make recommendations to the Secretary for Security and heads of the LEAs as and when necessary. During the report period, the Commissioner continued to give advice and recommendations on various procedural matters in the course of discharging his duties in overseeing and supervising the performance of the LEAs over their compliance with the requirements of the Ordinance. The Commissioner's recommendations to the Secretary for Security and the heads of the LEAs were summarized in Chapter 8 of the Report. The Commissioner also set out in Chapter 9 of the Report his views and recommendations on certain issues which have implications across the LEAs.

10. For those recommendations set out in Chapter 8 of the Report, the Security Bureau and the LEAs either have implemented them in full or are taking follow-up actions to address the Commissioner's concerns. The Secretary for Security has also revised the Code of Practice to give effect to the Commissioner's recommendations as appropriate. A summary of the Administration's responses to the key recommendations made by the Commissioner in the Report is set out at **Annex A**. A copy of the revised Code of Practice, issued by the Secretary for Security pursuant to section 63 of the Ordinance on 26 November 2012, is at **Annex B**. For those recommendations that would further require legislative amendments, the Administration is considering them in the context of the comprehensive review of the Ordinance.

CONCLUSION

11. The control regime under the Ordinance has continued to operate smoothly during the report period. The Administration will continue to closely monitor the operation of the regime, and fully co-operate with the Commissioner and the panel judges, with a view to better carrying out the objects of the Ordinance.

Security Bureau
November 2012

Annex A

Response of the Administration
to the key comments and recommendations made in the Annual Report 2011
of the Commissioner on Interception of Communications and Surveillance (the Commissioner)

	Comments and recommendations made by the Commissioner	The Administration's response
A.	**Recommendations to Secretary for Security (see Chapter 8)**	
1.	Time to make disciplinary award (paragraph 8.9)	
	The Commissioner noted that the Administration had accepted his recommendation set out in the Annual Report 2010 to amend paragraph 177 of the Code of Practice (COP) to require that an appropriate disciplinary award against an offending officer be made after the head of the LEA has apprised of the Commissioner's view at the conclusion of his review. The Commissioner requests the Administration to consider if there was a need to make corresponding amendment to section 54 of the ICSO.	● **Code of Practice amended.** Paragraph 177 of the revised COP issued on 28 November 2011 has been amended to stipulate that the LEAs should take into account any views that the Commissioner may have on the appropriate disciplinary action before taking any disciplinary action against an offending officer. The LEAs have been acting in accordance with this requirement since the implementation of the revised COP.

	Comments and recommendations made by the Commissioner	The Administration's response
B.	**Recommendations to the LEAs (see Chapter 8)**	
2.	Reporting of incidents, irregularities and non-compliance (paragraphs 8.11-8.14)	
	The Commissioner provided a time frame and reporting arrangement of incidents, irregularities and non-compliance for the LEAs to follow and requested the officer making the discovery of the event to make a record of discovery which should be signed with date and time by the discovering officer and by the senior officer to whom he reported the discovery. The failure on the part of LEA officers in complying with the time-frame and any time-line set by C/ICS may be visited with disciplinary action.	● **Recommendation accepted.** The LEAs will ensure compliance by its officers with the time-line set by the Commissioner in respect of non-compliance, irregularities or incidents and would consider taking disciplinary action for any failure by its officer to do so without reasonable cause or explanation.
3.	Inclusion of the rank of listeners in audit trail report (ATR) (paragraph 8.15)	
	The Commissioner recommended improvement to the presentation of the ATR to put the rank of the officers who had listened to the intercept product.	● **Recommendation accepted.** The inclusion of the rank of the listeners in the ATR was implemented in February 2011.

	Comments and recommendations made by the Commissioner	**The Administration's response**
4.	Reporting to the Commissioner under Paragraph 120 of the COP (paragraph 8.16)	
	The Commissioner advised that when reporting LPP cases to him under COP 120, the ATR attached to the notification to him should cover the period up to the date of notification or three weeks after disconnection of the facility concerned, whichever is earlier.	● **Recommendation accepted.** The requirement has been adopted by the LEAs.
5.	Submission of REP-11 report (paragraph 8.17)	
	The Commissioner recommended that both an REP-11 report and a section 57 report should be submitted to the panel judge in cases where the discontinuance of operation was related to an LPP or suspected LPP call or where there was heightened likelihood of obtaining LPP information.	● **Recommendation accepted.** The requirement has been adopted by the LEAs.
6.	Recommendations in connection with covert surveillance (paragraph 8.18)	
	(a) Sufficient background information should be included in the statement in writing so that the authorizing officer could make a well-informed and well-considered decision as to whether the	(a) **Recommendation accepted.** The LEAs are reminded to include sufficient background information in the statement in writing.

	Comments and recommendations made by the Commissioner	The Administration's response
	application should be granted or refused. (b) A system similar to the computerised device management system for handling devices for ICSO and non-ICSO purposes should be developed for the control of capable devices. (c) Various amendments were proposed to the device request forms, in particular, the addition of the time of signature by the officers concerned. (d) The computerised device management system should be enhanced to automatically capture the date and time of making a post-entry record and keep the history of all the post-entry records made.	(b) **Recommendation being considered.** The LEAs are taking actions to address the concerns of the Commissioner. (c) **Recommendation accepted.** The LEAs have taken actions to address the concerns of the Commissioner. (d) **Recommendation accepted.** The LEAs have taken actions to address the concerns of the Commissioner.
7.	Recommendations made upon review of LPP and JM cases (paragraphs 5.40, 5.90 and 8.19)	
	The Commissioner made the following two recommendations upon review of the LPP and JM cases in Chapter 5 of the Report -	

	Comments and recommendations made by the Commissioner	The Administration's response
	(a) The LEA should provide further and better training on the meaning of LPP information and on the proper and prudent attitude to take in handling possible LPP-related matters to its officers dealing with ICSO-related matters. (b) If the LEA considered that JM had been obtained, it should be more definite and expressly say so in the REP-11 report instead of saying "might" or "possible".	(a) **Recommendation accepted.** The LEA concerned will provide training to its officers to enhance their knowledge on LPP-related matters. (b) **Recommendation accepted.** The LEA concerned has been reminded to follow the Commissioner's advice.
8.	Recommendations made upon review of cases of non-compliance, irregularities and incidents (paragraph 8.20)	
	The Commissioner made the following three recommendations in the course of his review of the non-compliance, irregularities and incidents mentioned in Chapter 7 of the Report – (a) The LEA should disclose to the panel judge all the hitherto unknown names and alias of the subject known to the LEA (as soon as each crops up) with a corresponding "if known" declaration.	(a) **Code of Practice amended.** A new paragraph 114 of the revised COP issued on 26 November 2012 has been amended to add the requirement that LEAs should inform the relevant authority the identity and any relevant alias of the subject, if known to the

	Comments and recommendations made by the Commissioner	The Administration's response
		LEAs, in applying for a prescribed authorization with a corresponding "if known" declaration or as soon as practicable after the authorization or renewal is granted when the identity/relevant alias of the subject is known to the LEAs. With this new requirement in the COP, LEAs should report the identity/relevant alias to the relevant authority as soon as practicable when the identity/alias of the subject is known to the LEAs, and should not wait until the application for renewal of the prescribed authorization.
	(b) The LEA should look into the practice of listening and note-taking by its listeners and work out improvement measures so that it could be discerned from the listener's notes whether a call had been listened to but considered irrelevant or it had not been listened to.	(b) **Recommendation accepted.** The LEA concerned has reviewed the practices of listening and note-taking by its listeners and worked out improvement measures.
	(c) If any officer of the LEA fails to comply with the time-line set by C/ICS in his request for documents or information or report, it should be dealt with as a disciplinary matter.	(c) See response to item 2.

	Comments and recommendations made by the Commissioner	The Administration's response
C.	**Other Recommendations (see Chapter 9)**	
9.	To give express power to C/ICS and his designated staff to listen, to view and to monitor the products from interception and covert surveillance of their choice (paragraphs 9.2-9.15)	
	The Commissioner recommends that the ICSO be amended to give him and his designated staff express power necessary for listening to, viewing of and monitoring the products from interception and covert surveillance of their choice.	● **Recommendation being considered.** The Administration is considering the issue in the comprehensive review on the ICSO.
10.	Provision prohibiting or deferring examination (paragraphs 9.16-9.21)	
	The Commissioner recommends that consideration be given to have subsections (2) and (3) of section 45 repealed, which are related to the grounds for the Commissioner not to carry out an examination in respect of an application based on suspected interception or covert surveillance.	● **Recommendation being considered.** The Administration will look into the issue in the comprehensive review on the ICSO.

	Comments and recommendations made by the Commissioner	The Administration's response
11.	Names and aliases and the "if known" requirement (paragraphs 9.22-9.29)	
	The Commissioner recommends that Part 4 of Schedule 3 be amended to add in the "if known" requirement. Before the amendment to the Ordinance is effected and as a corollary, the Commissioner recommends that the COP be amended to include the "if known" requirement to apply to renewal applications for any of the statutory activities. He also recommends that a requirement be added in the COP for the LEAs to disclose all names and aliases of the subject that surface from time to time by way of a timely REP-11 report to the relevant authority, regardless whether they are considered as a significant change of information.	● See response to item 8(a).

Note: In respect of recommendations made by the Commissioner to the LEAs in relation to devices for non-ICSO purposes, the LEAs concerned have taken actions to follow up on the recommendations.

Annex B

Interception of Communications and Surveillance Ordinance

Code of Practice

Pursuant to Section 63 of the Interception of Communications and Surveillance Ordinance

GENERAL

This Code of Practice (this "Code") is issued under section 63 of the Interception of Communications and Surveillance Ordinance (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.

Balancing the "needs of public security or of investigation into criminal offences", and freedoms and rights

4. Article 30 of the Basic Law (BL 30) provides that –

> *"[t]he freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."*

5. Other provisions in Chapter III of the Basic Law protect other rights and freedoms. The underlying principle of the Ordinance is that any interference with any such rights and freedoms by the covert operations authorized and conducted under the Ordinance must be necessary for and

---

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 9 and 178 to 179 below.

proportionate to the purposes that such operations seek to achieve. These purposes are defined in section 3 of the Ordinance. For further guidance, see the part on "Conditions for Issue, Renewal or Continuance of Prescribed Authorization" in paragraphs 35 to 43 below.

Prohibition

6. Under the Ordinance, all public 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

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

7. Similarly, all public 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.

8. This Code sets out practical guidance for prescribed authorizations in respect of interception and covert surveillance referred to in paragraphs 6(a) and 7 respectively.

9. Law enforcement officers are also reminded to observe the requirements of the prescribed authorization fully in carrying out interception / covert surveillance 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, the whole operation should be stopped immediately except in circumstances where it is not feasible to do so in which case the whole operation should be stopped as soon as practicable, followed by a report to the

---

[3] Operations authorized under other enactments 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 47A, 47B and 47C of the Prison Rules (Cap. 234, sub. leg. A); and the control over the communications of inmates of mental hospitals with outsiders under the Mental Health Regulations (Cap. 136, sub. leg. A).

management of the department as soon as reasonably practicable. For guidance on situations where an operation is regarded as being or has been carried out without the authority of a prescribed authorization, see paragraph 149. The head of department should cause a report on any such irregularity to the Commissioner to be made.

INTERCEPTION OF COMMUNICATIONS

10. 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(6) of the Ordinance, it includes such data as the telephone numbers of the caller and the recipient, and other data that identify the source and the 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 warrant.

COVERT SURVEILLANCE

11. 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 in paragraphs 12 to 31 below.

12. 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 and activities of a professional or business nature.

13. A person has a reasonable expectation of privacy if (a) he, by his conduct, has exhibited a subjective expectation of privacy, that is, he has shown that he seeks to preserve something as private; and (b) his subjective expectation of privacy is one that society is prepared to recognize as reasonable, that is, the expectation, viewed objectively, is justifiable under the circumstances[4].

---

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

14. The following factors may be relevant in assessing whether an individual's privacy expectation is reasonable or not –

(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);

(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].

15. Paragraphs 16 to 26 provide further guidance in respect of covert surveillance with listening devices and optical surveillance devices.

Surveillance using listening devices

16. With regard to covert surveillance using a listening device, one of the factors that may be relevant in determining whether there is a reasonable expectation of privacy in respect of a communication is whether the communication would be audible to someone who is not a party to such communication, such as a passer-by, without the use of a sense-enhancing device. If not, the parties may reasonably expect privacy in their communication.

17. A person may reasonably expect that his communications would not be listened to or recorded by persons other than those who could hear the communications without the aid of a device. This is the case whether the communications take place in a public place or private premises. It should be noted that the expectation to be free from surveillance using a listening device is distinct from the expectation to be free from optical surveillance. A person can be visible to the public without forfeiting his right to the privacy of his communications. Persons having dinner in a restaurant have a reasonable expectation of privacy in relation to their conversations if the conversations are not audible to other members of the public patronizing the restaurant without

---

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

the aid of a listening device, even though the restaurant is a public place.

18. Conversely, a person speaking loudly from private premises may not have a reasonable expectation of privacy in respect of the words spoken, if these words can be heard without the aid of a device by persons outside the premises.

19. In considering whether a proposed surveillance operation with a listening device would intrude into a person's reasonable expectation of privacy and require authorization under the Ordinance, officers should consider carefully the circumstances of the operation, taking into account the factors in paragraph 14 above. Officers should only decide that the operation does not require authorization under the Ordinance if it is clear that the operation would not intrude into the person's reasonable expectation of privacy throughout the operation. This would cover the case, for example, of a person making a public speech in a public place, if the operation only seeks to monitor or record that public speech. Conversely, if the operation is also designed to capture that speaker's conversations with fellow speakers which are outside the hearing range of the audience, that part of the operation may intrude into the reasonable expectation of privacy of the speakers.

Optical surveillance

20. One of the factors that may be relevant in determining whether a person has a reasonable expectation of privacy with respect to covert surveillance carried out with the use of an optical surveillance device is whether the person's activities in question would be visible to other persons such as passers-by, without the use of a sense-enhancing device.

21. Accordingly, a person does not normally have a reasonable expectation of privacy in respect of optical surveillance when he is in an area open to the view of the general public. More specifically, under section 2(2) of the Ordinance, *"a person is not regarded as being entitled to a reasonable expectation of privacy ... in relation to any activity carried out by him in a public place …."*

22. In general, a person is likely to have a reasonable expectation of privacy if he has secluded himself in private premises, such as his home or office. However, where the individual is in plain view (for example, he is right before an open window) and is visible to the naked eyes of passers-by, an officer may observe the individual's activities without infringing the latter's

privacy, whether the observation is done with his naked eyes or a pair of ordinary binoculars. However, an individual standing before an open window would not be visible to the naked eye if, for example, he is in private premises on top of an isolated high-rise building or facing the open sea. In such circumstances, that individual would have a reasonable expectation to be free from being observed by others with their naked eyes. If a covert surveillance operation aims to observe or record that individual's activities using a sense-enhancing device (e.g. a long-range electronic optical surveillance device), it may intrude into his reasonable expectation of privacy.

23. As noted in paragraph 19 above in relation to listening devices, officers formulating a proposed operation with an optical device should think through the circumstances of the operation, taking into account the factors in paragraph 14 above. Bearing in mind that an individual's reasonable expectation to be free from optical surveillance may change with changes in circumstances as discussed in paragraph 22 above, officers should only decide that the operation does not require authorization under the Ordinance if it is clear that the operation would not intrude into the person's reasonable expectation of privacy throughout the operation.

24. 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.

25. As noted in paragraph 21, under section 2(2) of the Ordinance, a person is not regarded as being entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place. 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.

26. Under the Ordinance, the term "public place" is defined to mean any premises which are a public place as defined 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 apply to all such property of the kinds specified, whether owned by the Government, by a public department or by a private person."* Since "premises" is defined in the Ordinance to include any conveyance, "public place" may include a means of transport made available to the public.[6]

Type 1 and Type 2 Surveillance

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

28. 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 an optical or tracking device 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.

29. Section 2(3) of the Ordinance provides that 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. If an LEA has to apply to a panel judge for the issue of a prescribed authorization for Type 1 surveillance in these circumstances, it should state clearly in its application that the covert surveillance sought to be carried out by the LEA is regarded as Type 1 surveillance under section 2(3) of the Ordinance. The LEA should also

---

[6] Examples of "public places" under Cap. 228 are: (a) the pedestrian walkway inside a commercial complex (*HKSAR v 蔡就昌 (Choi Chau Cheung,* HCMA 380/2004*)*; (b) the podium at the Golden Bauhinia Square outside the HK Convention and Exhibition Centre (*HKSAR v Lau San Ching* [2003] 2 HKC 378). Where the public may have access to the common area of a public housing estate and use it as a thoroughfare, the area would fall within the definition of "public place" under Cap 228. However, the common parts of a building would not be considered as a public place if access is restricted to the occupiers and their licensees or invitees.

provide information in the supporting documents explaining why the proposed surveillance is likely to obtain information which may be subject to LPP.

30. "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 the exclusive use of the conveyance or object. A permission for entry obtained by deception is not regarded as permission.

31. 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 66 of the Ordinance.

PRESCRIBED AUTHORIZATIONS

32. 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

33. 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 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; and

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

In all circumstances, only officers whose substantive rank is not below the minimum rank (senior superintendent of police or equivalent) set out in the Ordinance may be appointed as authorizing officers for the purpose of considering applications for the issue of prescribed authorizations for Type 2 surveillance.

(c) Emergency Authorization

- the head of a department[7].

34. 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;

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

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

(c) the authorizing officer be involved in formulating the application.

Conditions for Issue, Renewal or Continuance of Prescribed Authorization

35. 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.

36. Section 2(1) of the Ordinance defines the term "serious crime". In relation to interception, serious crime means any offence punishable by a maximum sentence of not less than 7 years' imprisonment. In respect of covert surveillance, serious crime means any offence punishable by a maximum sentence of not less than 3 years' imprisonment or a fine of not less than HK$1,000,000. 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. It should be noted that the word "particular" in section 3 and other relevant provisions in the Ordinance seeks to make clear that any application for authorization must specify a "specific" serious crime or threat to public security.

37. The determination of what constitutes a threat to Hong Kong's public security is highly fact-based. Possible examples of such threats include activities connected with the illicit trafficking of weapons of mass destruction, terrorism-related activities, human trafficking, etc. Schedule 3 of the Ordinance requires an assessment of the impact, both direct and indirect, of the particular threat to the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong for applications made on grounds of public security. In connection with "indirect impact", this is a recognition of the fact that a threat to Hong Kong's public security need not be direct, and may be grounded in events which are distant but may indirectly harm Hong Kong's public security. It is the general understanding of the international community that the security of a jurisdiction may depend on the security of other jurisdictions. For example, the threats mentioned above may happen in one jurisdiction but could have an adverse impact on the security of another. 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. Grounds for believing that violent means are likely must be included in an application involving such activities. "Violence" does not cover minor scuffles or minor vandalism, etc. Furthermore, any applications for authorization must comply with the following statement made by the Secretary for Security during the Second Reading Debate of the Interception of Communications and Surveillance Bill on 2 August 2006 : *"Law enforcement agencies will under no circumstances undertake surveillance operations under the Bill on grounds of public security to achieve a political objective. ... The powers under the Bill after its passage will not be used for investigation of criminal offences that are yet to be created under Article 23 of the Basic Law."*

38. The key concept underlying section 3 of the Ordinance is the necessity and proportionality tests, which the various provisions in the section seek to embody[8]. In determining whether the operation is necessary and proportionate, the department has to:

(a) balance the immediacy and gravity of the particular serious crime or threat and the likely value and relevance of the information likely to be obtained against the intrusiveness of the operation;

(b) consider whether other less intrusive means are available; and

(c) consider other matters that are relevant in the circumstances.

39. The proportionality test involves balancing the intrusiveness of the operation on the subject and others who may be affected by it against the need for the operation.

40. Whenever possible, a less intrusive means should be used instead – for example, if the same objective can be achieved by a Type 2 surveillance instead of a Type 1 surveillance, or by overt means such as search warrants or court orders, the Type 2 surveillance or overt means respectively should be used as they are generally less intrusive to privacy.

41. An application for interception or covert surveillance which is

---

[8] Paragraphs 3.21 and 3.22 of the LRC Report on *Privacy: the Regulation of Covert Surveillance (2006)* elaborate on the proportionality test, the key points of which have been reflected in the provisions of section 3 of the Ordinance. Officers may wish to refer to the Report for further reference.

likely to result in the acquisition of information which may be subject to LPP should only be made in exceptional circumstances with full justifications. Full regard should be paid to the particular proportionality issues that such an operation would raise. The application must include an assessment of how likely it is that such privileged information will be obtained. For more details about the measures that should be put in place to protect such privileged information, see the part on "Protection of LPP information" in paragraphs 119 to 127 below.

42. As regards the other relevant matters that may be taken into consideration by the relevant authority, 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).

43. 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 for 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

44. The applicant for all applications to be 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.

45. Apart from the information required to be provided under the Ordinance, all information known to the applicant to be relevant to the determination of an application should be provided in the affidavit / affirmation or statement for the relevant authority to make a balanced decision. All applications should be sufficiently justified. The applicant and the officer approving the submission of the application (paragraphs 53 and 58 below refer) should not base their judgement on the complainant's mere suspicion, or on their personal experience / knowledge unless specifically mentioned with full particulars in the affidavit / affirmation or statement in support of the

application. The fact and particulars of any previous application relating to the subject person and/or telecommunications service of the proposed authorization that are required to be disclosed to the relevant authority by virtue of Schedule 3 to the Ordinance should be mentioned in the affidavit / affirmation or statement supporting the application. 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. Full and frank disclosure of any previous authorizations on the same subject(s) in respect of the same case which had been allowed to lapse (instead of being discontinued and revoked before their expiry) and the reasons for allowing them to lapse should also be provided. (See also paragraph 167.) All applications except oral applications should be made in writing, and should be signed by the applicant. In this connection, officers are reminded that in no case should they wilfully make a false statement in the affidavit / affirmation or statement required to be provided under the Ordinance, or provide information which is misleading in a material particular (i.e. of a kind which might affect the decision). It is an offence to wilfully make a false statement in an affidavit / affirmation or statement, and an authorization obtained on the basis of such false information might be determined to be invalid and any operation based on the authorization might be determined to have been conducted without the authority of an authorization in the circumstances described in paragraph 149.

46. If a previous application relating to the same interception / covert surveillance operation has already been refused, an officer must not submit another application for the same authorization unless there has been a material change in circumstances or there is additional information to support the application.

47. 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. To allow the relevant authority to critically assess whether the duration sought is appropriate, applicants have the duty to provide sufficient grounds in their supporting affidavit / affirmation or statement in writing to justify the requested duration. The term “period” should refer to a specified time duration. The period cannot exceed the maximum statutory period. In the case of covert surveillance, the duration sought may include a “lead time” for testing the serviceability of the devices to be drawn but the duration of the “lead time” must be reasonable. Apart from the testing of serviceability, “lead time” might also be required for the devices to be brought

to the place where surveillance is to be conducted or for early installation of devices in the targeted premises. To facilitate the relevant authority's consideration of the effective starting time for a prescribed authorization sought, applicants should explain clearly in their applications why a "lead time" is required.

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

49. To enable the relevant authority to consider applications in context, the supporting affidavit / affirmation or statement in writing must specify clearly what type of interception or covert surveillance is 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 or will target.

50. Furthermore, the category of authorization (i.e. subject-based, service-based, premises / address-based, or object-based) being applied for should be expressly stated in the affirmations / affidavits or statements supporting the application. (See paragraphs 106 to 115 below.) In particular, in the case of an application for interception, where a service-based authorization involving more than one facility is sought, the details of each and every facility sought to be covered by the authorization should be provided in separate consecutive schedules attached to the draft authorization so that the panel judge may make a determination in respect of each facility identified on the respective schedule; and where a subject-based authorization is applied for, the application should clearly state that the authorization sought for covers interception of facilities which the subject "is using or is reasonably expected to use".

51. For the same investigation or operation, a single application may

cover more than one subject. This is possible if the individuals concerned are involved in the same crime or threat and it is necessary to monitor their communications or activities during the same period of time. In applying for authorization covering such specified subjects, the applicant should make an assessment on the proportionality and necessity tests having regard to the case of each of these subjects. 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

52. This part 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 the Issue of Judge's Authorization for Interception or Type 1 Surveillance

53. 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**.

54. 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 in Part 1 or 2 of Schedule 3 to the Ordinance (as the case may be). The affidavit / affirmation should as far as possible be sworn / affirmed 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

55. The panel judge will deliver in writing his determination[9], and will

[9] 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 will arrange for the hearing to be audio-taped, or will cause the

deliver 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

56. Section 10 of the Ordinance provides for the duration of a judge's authorization. Paragraph 47 above is relevant.

Renewal of Judge's Authorizations

57. If a judge's authorization in force has to be renewed, a renewal application must be made before the authorization ceases to have effect. The renewal will take effect at the time when the judge's authorization would have ceased to have effect but for the renewal, i.e. the time of expiry of the authorization sought to be renewed. A judge's authorization may be renewed more than once.

Application for Renewal of Judge's Authorization

58. 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).

59. Other detailed arrangements in respect of the affidavit / affirmation as set out in paragraphs 45 and 54 above apply. Any renewal of the same authorization for more than five times should be reported to the Commissioner. When different authorizations of the same case are combined in an application for renewal, the counting should start from the earliest authorization, irrespective of any subsequent discontinuance of operations in respect of facilities contained in that authorization. Where different authorizations of the same case have not been combined, such authorizations should be treated as

---

information to be recorded in writing. The officer should also make a note of the hearing to record the directives given by the panel judge.

stand-alone cases.

Determination of Renewal of Judge's Authorization

60. The panel judge will deliver in writing his determination, and will deliver 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

61. Section 13 of the Ordinance provides for the duration of a renewal of a judge's authorization. Paragraph 47 above is relevant.

Issue of Executive Authorizations

62. This part 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.

63. 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 33(b) above.

Applying to a panel judge for an authorization for Type 2 surveillance

64. Where there is a likelihood of a Type 2 surveillance operation obtaining information which may be subject to LPP, the Type 2 surveillance is regarded as Type 1 surveillance under section 2(3) of the Ordinance. In these circumstances, the LEA must apply to a panel judge for a prescribed authorization for Type 1 surveillance even though the covert surveillance is otherwise Type 2 surveillance. See paragraph 29 above. On the other hand, section 2(4) of the Ordinance provides that an officer may apply for the issue or renewal of a prescribed authorization for Type 2 surveillance 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 to a panel judge under section 2(4) if the operation would involve both Type 1 and Type 2 surveillance, thus obviating the need to apply to both a panel judge and an authorizing officer for all the authorisations required for the same operation.

65. In addition, special circumstances of a Type 2 surveillance operation may render it particularly intrusive, for example –

- 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 to protect his privacy 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 to a panel judge instead of an authorizing officer for a prescribed authorization for Type 2 surveillance under section 2(4) of the Ordinance. If an LEA wishes to make such an application, it should state in the application that it is made under section 2(4) of the Ordinance, and provide full justifications and detailed information in the supporting documents explaining why the application is made under that subsection.

Application for Issue of Executive Authorization

66. An application for executive authorization shall be made in writing (**COP-8** at **Annex**) 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. A sample checklist as to the types of information that may need to be included is at **COP-9** at **Annex**.

67. Should the case involve participant monitoring in Type 2 surveillance, the consent of the participating party, unless he is an officer of a department, should be obtained prior to the operation taking place, which, where practicable and without causing risks to the safety of the party concerned or prejudicing the operation, should be in writing, and this should be so indicated in the application.

Determination of Application for Executive Authorization by the Authorizing Officer

68. Authorizing officer should take a critical approach when considering applications, including whether the application is fully justified and

whether the duration sought is reasonable. He should not approve an application as a matter of course or consider the application solely in light of his knowledge of the case in question. Where necessary, he should seek clarification and explanation from the applicant before he comes to any determination. 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**).

69. 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 35 to 43 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 or paralegals), etc. may be relevant (paragraph 65 above). In particular, special attention should be paid to the assessment of the likelihood that information which may be subject to LPP will be obtained. If LPP information is likely to be obtained through the proposed covert surveillance operation, an application for Type 1 authorization from a panel judge should be made (paragraph 29 above).

Duration of Executive Authorization

70. Section 16 of the Ordinance provides for the duration of an executive authorization. Paragraph 47 above is relevant.

Renewal of Executive Authorization

71. If an executive authorization in force has to be renewed, a renewal application must be made before the executive authorization ceases to have effect. The renewal will take effect at the time when the executive authorization would have ceased to have effect but for the renewal, i.e. the time of expiry of the authorization sought to be renewed. An executive authorization may be renewed more than once.

Application for Renewal of Executive Authorization

72. An officer of the department concerned may apply to an authorizing officer of the department for renewal of an 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). A sample checklist of the information that may need to be provided is at **COP-13** at **Annex**.

73. 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

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

Duration of Renewal of Executive Authorization

75. Section 19 of the Ordinance provides for the duration of a renewal of an executive authorization. Paragraph 47 above is relevant.

Emergency Authorizations

76. This part 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

77. 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 should be satisfied that the gravity of the case justifies the emergency authorization.

78. 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.

79. Unless the oral application procedures set out in paragraphs 90 to 105 below apply, the application for emergency authorization shall be in writing (**COP-20** at **Annex**) and supported by a statement in writing made by the applicant detailing the facts which are relied upon to obtain the emergency authorization. See sample checklist at **COP-9** at **Annex** for reference as to the types of information that may need to be included. The statement must set out the reason for making the application for emergency authorization and contain the information set out in Part 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

80. The head of the department shall deliver in writing his determination (**COP-21** or **COP-22** at **Annex**). He shall not issue the emergency authorization unless he is satisfied that the emergency conditions (see paragraph 77) and the conditions for issuing the authorization set out in section 3 of the Ordinance (see paragraphs 35 to 43 above) are all met. In issuing an emergency authorization, the head of department should impose a condition, pursuant to section 32 of the Ordinance, that the applicant or any other authorized officer of the department shall, as soon as practicable, and in any event during the validity of the emergency authorization, bring to the attention of the head of department as well as any panel judge any –

(a) initial material inaccuracies; or

(b) material change of circumstances upon which the emergency authorization was granted,

which the applicant becomes aware of during its period of validity. The head of department should also have regard to special considerations such as protection of LPP in approving an application for emergency authorization, and to impose additional conditions where appropriate.

Duration of Emergency Authorization

81. Section 22 of the Ordinance provides for the duration of an emergency authorization. Paragraph 47 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 time.

Application for Confirmation of Emergency Authorization

82. 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, and in any event within the period of 48 hours beginning with the time when the emergency authorization is issued, irrespective of whether the interception / covert surveillance has been completed or not. Unless directed otherwise, the application for confirmation should be made by the same officer who has applied for the emergency authorization.

83. The application should be made in writing (**COP-3** at **Annex**). 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 79 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 provided for the purpose of the application for the issue of the emergency authorization).

84. It is essential that application for confirmation of an authorization be made within 48 hours of the issue 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 interception / covert surveillance.

85. 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.

86. Any failure to apply for confirmation of an emergency authorization is a grave irregularity and will be viewed most seriously. Apart from the destruction of information obtained by carrying out the interception / covert surveillance (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

87. 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.

88. 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" in section 24(3) has the same meaning as set out in paragraph 84.

89. 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

90. This part 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 or executive authorization, under Division 5 of Part 3 of the Ordinance[10].

Oral Application for Prescribed Authorizations

91. An application for the issue or renewal of a prescribed authorization 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 make an oral application to the same relevant authority as for a written application. For example, in an urgent case involving serious bodily harm, although there is not enough time to prepare the supporting affidavit / affirmation in writing, it may still be practicable for an officer to appear before a panel judge to make an oral application for an authorization to carry out interception. Another example is where the written statement has been prepared, but the applicant cannot appear before the authorizing officer in person due to, say, very adverse weather conditions or bad road conditions but may contact him by telephone. Such an oral application could be justified if the operation is time-critical and cannot wait until the weather or road conditions return to normal. Also, if arrangements have to be made for the applicant to take part in a participant monitoring Type 2 surveillance operation that has to be carried out very soon and he cannot afford the time to submit a written application due to the urgency of the case, an oral application may be made.

92. The oral application procedures under the Ordinance should only be resorted to in exceptional circumstances and in time-critical cases where the normal written application procedures cannot be followed.

93. 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 if it is made orally in person or made by telephone, video conferencing or other electronic means by which*

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

words spoken can be heard (whether or not any part of the application is made in writing)".

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

95. 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. The applicant should also make a note of the proceedings. 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 application for confirmation of the authorization.

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

96. 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, and in any event within the period of 48 hours beginning with the time when the prescribed authorization or renewal is issued or granted. Unless directed otherwise, the original applicant of the oral application should make the application for confirmation.

97. The application shall be made in writing and shall 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 would 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 sets out all the information provided during the initial oral application, whether orally or in writing, and verifies that such information was that provided during the oral application, as well as a record in writing setting out the determination delivered orally in respect of the initial oral application. In case of any discrepancy in the records made by the relevant authority and the applicant, the decision as to which version to adopt would rest with the relevant authority.

98. The application documents for confirmation of judge's

authorization, executive authorization and emergency authorization granted in respect of oral applications are set out respectively at **COP-5, COP-16 and COP-4** at **Annex**. It is essential that an application for confirmation be made within 48 hours. Otherwise, similar considerations as in paragraphs 84 to 86 above apply.

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

99. In case where the application for confirmation is made to a panel judge, the panel judge will deliver in writing his determination, and will deliver the determination and the certified copy of the application, the affidavit / affirmation and other supporting documents submitted with the application to the applicant.

100. In the case of executive authorization, after considering an application for confirmation of an executive authorization or its renewal granted upon oral application, the authorizing officer will deliver in writing his determination (**COP-17** or **COP-18** at **Annex**).

101. The Ordinance provides that the relevant authority shall not confirm the prescribed authorization or renewal unless he is satisfied that the relevant conditions provision as defined under section 27(6) of the Ordinance[11] has been complied with in the issue or granting of the prescribed authorization or renewal. (See also paragraphs 35 to 43 above.)

102. Where 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" in section 27(3) has the same meaning as set out in paragraph 84.

103. 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 Procedures for Application for Confirmation of Emergency Authorization Issued as a result of Oral Application

[11] Meaning section 9(2), 12(2), 15(2), 18(2) or 21(2)(b), as the case may be.

104. In the case of an emergency authorization issued as a result of an oral application, compliance with the confirmation requirements of sections 23 and 26 of the Ordinance would involve a two-step process, i.e. an application to the head of the department concerned for confirmation of the oral application in respect of the emergency authorization pursuant to section 26 of the Ordinance, followed by a separate application to a panel judge for confirmation of the emergency authorization pursuant to section 23 of the Ordinance in accordance with the procedures set out in paragraphs 82 to 89.

105. To obviate the need for two separate applications to be made as described above, section 28 of the Ordinance provides for special arrangements regarding the confirmation of an emergency authorization issued as a result of an oral application under which it is unnecessary to make a separate application to the head of department under section 26 of the Ordinance. This procedure should be followed unless the head of department specifically requests that the two-step confirmation procedure be followed when he issues an emergency authorization on an oral application, or when no operation has been carried out pursuant to the emergency authorization[12]. For the procedure under section 28 of the Ordinance, the applicant should prepare an application as per the format at **COP-4** at **Annex** and an affidavit / affirmation in support. The application should be made in writing and supported by the documents set out in section 28(1)(b) of the Ordinance (broadly similar to those set out in paragraph 97 above, including an affidavit / affirmation stating and verifying all the information provided to the head of department concerned under section 20(2)(b) or section 25(3)). Other arrangements regarding the application for confirmation of emergency authorization, and the determination of such an application, as set out in paragraphs 82 to 89 are applicable.

Implementation Aspects

What a prescribed authorization authorizes

Interception

106. A prescribed authorization for interception may be address-based (section 29(1)(a)(i) of the Ordinance, i.e. an authorization in respect of the specific premises or address(es) set out in it), service-based (section 29(1)(b)(i),

[12] Where no operation has been carried out pursuant to an emergency authorization, no application for confirmation is required to be made to a panel judge under section 23(1). Section 28 is therefore inapplicable and the application for confirmation should be made under section 26 instead.

i.e. an authorization in respect of the specific facilities set out in it) or subject-based (section 29(1)(a)(ii) and (b)(ii), i.e. in the case of telecommunications interception operations, involving the "reasonably expected to use" clause). Where necessary, an officer may apply for both an address- or service-based authorization and a subject-based authorization in respect of the same case.

107. A subject-based authorization for interception authorizes the interception of telecommunications made to or from any telecommunications service that the subject "is using or is reasonably expected 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 reasonably expected 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.

108. An applicant should make the best endeavours to first establish the telecommunications service or postal address (as the case may be) that is being used by the subject and apply for a service-based or address-based authorization if such information is available and this type of authorization is sufficient for the purpose. If need be, an application can be made for a subject-based authorization instead of, or in addition to, a service- or address-based authorization, with the known facilities or addresses provided as far as possible. An application for a subject-based authorization should only be made with strong justifications where other means of investigation, including service-based interception, 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 if this is a relevant consideration.

109. 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 reasonably expected 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 reasonably expected to use the telephone number, email address, postal address etc. The requirement "is using or is reasonably expected to use" means that it would be inappropriate to include a telecommunications service or postal address the subject may only use incidentally. An officer should not apply to an approving officer for the inclusion of any facility which, for application for an authorization for interception, was included in a schedule of the draft authorization, but had been refused authorization by a panel judge. In such case, if interception of the facility in question is considered necessary, a fresh application for a service-based authorization should be made.

110. Arrangements should be made for the determination of an application for inclusion of one or more facilities pursuant to a subject-based authorization to be reported to a panel judge, whether the determination is in favour of the applicant or not. Facilities added pursuant to a subject-based authorization ("added facilities") should be recorded separately from those authorized by the panel judges, i.e. those contained in the schedules attached to the authorization ("scheduled facilities"). On the expiry or revocation of the authorization, interception shall not be carried out on both the scheduled facilities and the added facilities. The head of department should ensure that arrangements are made to keep a proper record of the identifying details of the added facilities. The fact that an authorization for interception containing the "reasonably expected to use" clause has been granted does not mean that subsequent renewals granted by a panel judge automatically embrace such a clause, unless the panel judge has expressly stated so in the renewed authorization. Moreover, if the "reasonably expected to use" clause was rejected in a previous authorization, the LEA concerned should not seek the inclusion of the "reasonably expected to use" clause in subsequent applications for renewals unless there are new grounds to support it.

Covert surveillance

111. 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)).

112. A subject-based authorization for covert surveillance caters for situations where the subject has to be kept under close observation for a continuous period, or 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.

113. Even where there is a subject-based authorization for covert surveillance, Type 1 surveillance may only be carried out on particular 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 of the premises on which Type 1 surveillance is carried out under a subject-based authorization.

Report of Identity of the Subject

114. If known, an application for a judge's authorization or an executive authorization should include, in the affidavit / affirmation or statement supporting the application, the identity of any person who is to be the subject of the interception / surveillance and any alias that he uses which is relevant to the investigation. If the identity or such an alias is made known to the applicant after the authorization has been granted and the authorization or its renewal is still valid, the identity or alias of the subject should be reported to the relevant authority as a material change of circumstances for his consideration as soon as practicable.

Other points to note

115. An authorization may be framed with reference to the particular premises, address, service and / or subject. Where the authorization is framed in relation to the communications or activities of the subject at the specified premises (i.e. "subject-based and premises-based"), the interception or covert surveillance may only be directed at the subject at the specified premises, and may not be carried out, say, on the subject when he is outside the premises. In other words, the premises specified would circumscribe the subject-based authorization. When there is indeed a need to carry out an operation both on all persons within a specified premises and on a subject in other premises, applicants should consider submitting separate applications to avoid possible confusion. Moreover, in describing the ambit of a premises-based authorization under an application, care must be exercised to ensure that the ambit would not become too wide or without limit.

116. 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 reasonably 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.

117. A prescribed authorization, other than an executive authorization, may also 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 reasonable assistance for 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.

118. Sections 29(6) and (7), and 30 of the Ordinance cover other matters which are essentially incidental to the authorization. Nonetheless, officers are reminded that any such conduct should only be confined 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 officer performing such conduct may not be protected by the immunity in respect of civil and criminal liability under section 65.

Protection of LPP information

119. 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 risk of inadvertently obtaining information that may be subject to LPP during such operations. Section 31 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.

120. 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 that may be 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 31 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, and justification for the proposed interception / covert surveillance should be given in the affirmation / affidavit supporting the application.

121. Any information that is subject to LPP will 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 of initial screening by separate dedicated units is covert surveillance involving participant monitoring where, for the safety or well-being of the participants participating in the conversation (including the victims of crimes under investigation, informers 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 relevant authority, 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. The Commissioner should be notified of interception / covert surveillance operations that are likely to involve LPP information as well as other cases where LPP information has been obtained inadvertently. On the basis of the department's notification, the Commissioner may, inter alia, review the information passed on by the dedicated units to the investigators to check that it does not contain any information subject to LPP that should have been screened out. The Commissioner should also be notified of cases where information which may be the contents of any journalistic material has been obtained or will likely be obtained through interception or covert surveillance operations.

122. To ensure compliance with the requirements set out in paragraphs

119 to 121 above, an officer at or above the rank of assistant commissioner of police (or equivalent) shall cause random checks to be conducted on the materials provided by the dedicated units to the investigators, to see if any materials containing information subject to LPP have been provided to the investigators.

123. Where, further to the issue or renewal of a prescribed authorization, if the officer who is in charge of the interception / covert surveillance concerned becomes aware that the subject of the interception / covert surveillance has been arrested, and he forms an opinion that it is no longer necessary for the interception / covert surveillance to be continued after the arrest, he shall cause the interception / covert surveillance to be discontinued and shall, as soon as reasonably practicable after the discontinuance, cause a report to be provided to the relevant authority for revocation of the authorization in accordance with section 57(3). (See also paragraphs 158 to 168 below.) If, on the other hand, he forms an opinion that the interception / covert surveillance should continue, 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 interception / covert surveillance and cause a report to be provided to the relevant authority under section 58 of the Ordinance. In the case of an emergency authorization which will have been issued by the head of department concerned, the report should also be copied to the panel judges as soon as reasonably practicable.

124. On receiving the report submitted in accordance with section 58 of the Ordinance, the relevant authority will revoke the prescribed authorization if he considers that the conditions for the continuance of the prescribed authorization are no longer met.

125. 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 170 below.)

126. In the case of postal interception or covert surveillance, if the client enjoying the privilege is the defendant in a court action, and wishes the record of the communication to be used as evidence, he can waive his privilege and ask

the prosecutor to produce it. Where the client is not a defendant in the court proceedings, or where the client 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 will refuse disclosure of this part of the covert surveillance or postal interception product to them should the client refuse to waive his privilege.

127. 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

128. The safety of any device to be used, including its 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.

129. 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 property 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 unless the object is a tracking device in which case an authorization for the use of such a device should be separately applied for. Permanent removal of any of the contents from the packet is also not allowed. (See also paragraph 9.)

130. There should be suitable control mechanisms in respect of interception / covert surveillance conducted under the Ordinance to guard against possible abuse. 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 of police or above (or equivalent). The officers of the department (in the latter case, the supervisory staff) should ensure that a report to record details of the examination is completed and duly signed by officers carrying out or witnessing the examination. Such report

should be made available for inspection by the Commissioner.

131. Departments should also ensure that proper records with clear description of the exact usage are kept on the inventories and movement of devices to minimize the possibility of unauthorized usage. Moreover, to minimize the chance of possible abuse in the use of the devices by frontline officers for unauthorized purposes, only in justified circumstances should LEA officers be allowed to keep the surveillance devices. For example, where an anticipated meeting of the target has been postponed or does not materialize, the LEA officers concerned should, where practicable, return the relevant surveillance devices during the interim period before the target's next meeting has been confirmed. When a particular type of surveillance devices is no longer required for the surveillance operation authorized by an authorization, it should not be included in the affidavit supporting an application for renewal. The change of circumstances should also be clearly stated in the affidavit. On the other hand, if a new or additional type of devices is required, a fresh application instead of a renewal application should be made.

132. Individual officers should also return their devices in hand as soon as it is firmly established that no further covert surveillance will be conducted even though the related authorization is still in force. The officer-in-charge of the covert surveillance operation and the officer-in-charge of the device store(s) or registry designated by the department concerned for controlling the return of surveillance devices should pay attention to the expected time of discontinuance of the covert surveillance or the expiry date of individual authorization so as to ensure that loaned items will be returned to the device store(s) or registry as soon as reasonably practicable and officers will not keep any outstanding items after the conclusion of the covert surveillance operation.

133. Officers-in-charge of the covert surveillance 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.

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

135. The same minimization principle applies to any interference with property. While a prescribed authorization may authorize interference with property, this is allowed 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 any interference with property right, and is also essential for preserving the secrecy of the interception / covert surveillance operation. 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 the Chief Executive under section 50 of the Ordinance or make a recommendation to the department concerned under section 52 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

136. As a matter of policy, surveillance devices should not be left in the target premises after the completion or discontinuance of the covert surveillance operation, 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 yet been retrieved. In all cases, at the expiration of the authorization, the officer-in-charge of the covert surveillance 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.

137. 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

138. The general rules on the application for issue and renewal of authorizations as set out paragraphs 44 to 51 are applicable to the application for device retrieval warrants.

Application for Device Retrieval Warrant

139. Section 33 of the Ordinance applies to the application for device retrieval warrants.

140. 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

141. Section 35 of the Ordinance provides for the duration of a device retrieval warrant. Paragraph 47 above is relevant.

General Provisions of Device Retrieval Warrant

142. Sections 36 and 37 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 the application so that it could be so authorized. While no specific authorization for other incidental conduct set out in section 37 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 after completion or discontinuance of the covert surveillance operation.

Report following retrieval or other circumstances when the Device Retrieval Warrant no longer has effect

143. Once the device retrieval warrant is executed and the device authorized to be used under the prescribed authorization has been retrieved, the warrant will cease to have any legal effect. Also, in cases where any information provided to support an application for the issue of a device retrieval warrant (such as particulars of the premises or object from which the device is to be retrieved) is incorrect, and the error is not a minor defect within the meaning of section 64 of the Ordinance, the device retrieval warrant will also have no legal effect. In these cases, the officer-in-charge of the covert surveillance operation should cause a report to be provided to the panel judges, informing them of the circumstances leading to the device retrieval warrant ceasing to have any legal effect.

SAFEGUARDS

INDEPENDENT OVERSIGHT AUTHORITY

Functions of the Commissioner

144. 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

145. The Commissioner may conduct reviews in 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, the failure to apply for confirmation of a 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 departments relating to interception / covert surveillance operations in which materials consisting of LPP information 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.

146. 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.

147. 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

148. A person may apply to the Commissioner for an examination under section 43 of the Ordinance. Since the applicant would not be required to "prove" his allegation, it is important for a department to cooperate fully with the Commissioner in carrying out his examination (see paragraph 150).

149. The Commissioner will conduct an examination applying the principles applicable by a court on an application for judicial review to determine whether the alleged operation 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, for example –

(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 interception / covert surveillance 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 relevant authority.

150. 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 result in disciplinary actions and the incident may be reported to the Chief Executive.

151. 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, or, 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.

152. 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.

153. 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 will 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

154. Under section 48(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 of 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

155. 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 or

device retrieval warrants. 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.

156. If any instance of non-compliance is identified during such reviews or an officer of the department is otherwise made aware of it, arrangements should be in place for notifying the non-compliance to the Commissioner in the first instance, followed by a full report in accordance with section 54 of the Ordinance. Such report should include the details of the case, details of the investigation and the remedial measures taken, where applicable. Departments should also preserve relevant materials, where available, for subsequent enquiry to be performed by the Commissioner. For example, where the non-compliance relates to the execution of an authorization for telecommunications interception, this should include materials relating to the particulars of the intercepted facilities, the affected person, as well as the duration of the interception at issue.

157. The head of department shall also designate a reviewing officer under section 56(2) of the Ordinance to keep under review the performance by the authorizing officers of any function under the Ordinance. This 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

158. If an officer conducting reviews under section 56(1) or section 56(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.

159. An officer must be assigned to be in charge of a covert operation for the purpose of section 57(2) of the Ordinance. 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.

160. The officer for the purpose of section 57(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.

161. Where any interception or covert surveillance operation 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. Where the interception or covert surveillance operation is discontinued shortly before the expiry of the relevant authorization such that the discontinuance report would reach the relevant authority after the expiry of the relevant authorization, the officer should add a note to the discontinuance report stating that the discontinuance report is submitted in accordance with section 57 of the Ordinance even though the prescribed authorization has expired or will have expired by the time the report reaches the relevant authority. Departments should give the full reasons with specific and clear description of the ground for discontinuance and / or relevant circumstances leading to the discontinuance in the report. If there has been any unauthorized interception or covert surveillance or any irregularity leading or contributing to the discontinuance, this should be clearly stated in the discontinuance report.

162. A ground for discontinuance of an interception / covert surveillance 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 an interception / covert surveillance 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 interception / covert

surveillance operation, all the information sought has already been obtained, or the interception / covert surveillance operation is not productive or is no longer expected to be productive, etc. In the case of 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 continuance of the interception / covert surveillance disproportionate to the purpose sought and hence discontinuance is required.

163. For interception operations, where the officer conducting a review or the officer-in-charge of the operation considers that interception of any of the scheduled facilities as specifically authorized for interception should cease, but interception of other facilities under the same authorization should nevertheless continue, the cancellation of the former type of scheduled facilities should be reported to the panel judges.

164. For subject-based interception, it is incumbent on the officer-in-charge to keep under review the list of added facilities with a view to deleting from the list any telecommunication service or address etc. that the subject is no longer using or is not reasonably expected to use. The cancellation and the reason for it should be properly recorded. As the authority for approving the cancellation of added facilities under subject-based interception rests with the LEA concerned (paragraph 109 refers), the panel judges will not be involved in the process. However, a report should be made to the panel judges on the cancellation as soon as reasonably practicable to keep them informed, unless no other facility (added facility or scheduled facility) remains under the authorization after such cancellation, in which case the discontinuance of the interception should be reported under section 57 for the purpose of seeking revocation of the authorization.

165. 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 yet 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 paragraphs 136 to 137)). 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.

166. The forms for reporting on the discontinuance of an operation under a prescribed authorization are set out respectively at **COP-7, COP-19** and **COP-23** at **Annex**. Reports of discontinuance of operation under emergency authorization should also be copied to the panel judges as soon as reasonably practicable, besides the head of department concerned.

167. In case where an authorization granted is simply allowed to lapse on expiry without earlier discontinuance, full and frank disclosure of the lapsed authorization and reasons for allowing it to lapse, instead of early discontinuance, should be provided to the relevant authority in any subsequent application which involves the same subject in respect of the same case.

168. In the case of interception / covert surveillance which the LEA concerned assesses should continue after the arrest of the subject, if the relevant authority considers that the conditions for the continuance of the prescribed authorization are no longer met on receiving the report submitted by the LEA in accordance with section 58 of the Ordinance, he will revoke the prescribed authorization (see paragraphs 123 and 124 above). In anticipation of this possibility, LEAs should make arrangements to ensure that the interception / covert surveillance in question can be discontinued within a short period of time in case the prescribed authorization is indeed revoked.

SAFEGUARDS FOR PROTECTED PRODUCTS

169. Where any protected product[13] has been obtained pursuant to any prescribed authorization, the head of the department should make arrangements to ensure that the requirements in section 59 of the Ordinance are satisfied.

170. As pointed out in paragraph 125 above, where any protected product contains any information that is subject to LPP, the head of the department concerned should ensure that any part of 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

[13] Copies of protected 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.

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

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

172. Departments should, on the basis of their mode of operation, set up system(s) to document the information obtained from interception / covert surveillance authorized under the Ordinance, with restricted access to the different types of information depending on the confidentiality level, and keep a proper paper trail on access, disclosure and reproduction.

173. 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.

174. Notwithstanding the general non-admissibility policy, section 61(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

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

176. 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.

177. Section 60 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

178. 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. The LEAs should take into account any views that the Commissioner may have on the appropriate disciplinary action before taking any disciplinary action against an offending officer.

179. 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 Security Bureau.

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

* * * * *

Secretary for Security
November 2012

Annex

LIST OF PRESCRIBED FORMS

Prescribed Forms for submission to Panel Judge

Fresh Application – interception / Type 1 surveillance

COP-1 Application for an authorization for interception / Type 1 surveillance (section 8(1))

Renewal Application – interception / Type 1 surveillance

COP-2 Application for renewal of an authorization for interception / Type 1 surveillance (section 11(1))

Confirmation of emergency authorization for interception / Type 1 surveillance

COP-3 Application for confirmation of an emergency authorization for interception / Type 1 surveillance (section 23(1))

Confirmation of emergency authorization for interception / Type 1 surveillance issued upon oral application

COP-4 Application for confirmation of an emergency authorization for interception / Type 1 surveillance issued upon oral application (section 23(1) and section 28(1))

Confirmation of an authorization for interception / Type 1 surveillance issued / the renewal of an authorization for interception / Type 1 surveillance granted upon oral application

COP-5 Application for confirmation of an authorization for interception / Type 1 surveillance issued / the renewal of an authorization for interception / Type 1 surveillance granted upon oral application (section 26(1))

Application for a device retrieval warrant

COP-6 Application for a device retrieval warrant (section 33(1))

Report on the discontinuance of interception / Type 1 surveillance carried out under a prescribed authorization

COP-7 Report on the discontinuance of interception / Type 1 surveillance carried out under a prescribed authorization (section 57(3))

Prescribed Form for submission to/use by Authorizing Officer

Fresh Application – Type 2 surveillance

COP-8 Application for an executive authorization for Type 2 surveillance (section 14(1))

COP-9 Statement in writing in support of an application for an executive authorization for Type 2 surveillance (section 14(2))

COP-10 Executive authorization for Type 2 surveillance (section 15(1)(a))

COP-11 Refusal of application for an executive authorization for Type 2 surveillance (section 15(1)(b) and (3)(b))

Renewal Application – Type 2 surveillance

COP-12 Application for renewal of an executive authorization for Type 2 surveillance (section 17(1))

COP-13 Statement in writing in support of an application for renewal of an executive authorization for Type 2 surveillance (section 17(2))

COP-14 Renewed executive authorization for Type 2 surveillance (section 18(1)(a) and (3)(a))

COP-15 Refusal of application for renewal of an executive authorization for Type 2 surveillance (section 18(1)(b) and (3)(b))

Confirmation of executive authorization / renewal of executive authorization issued upon oral application

COP-16 Application for confirmation of an executive authorization for Type 2 surveillance issued / the renewal of an executive

authorization for Type 2 surveillance granted upon oral application (section 26(1))

COP-17 Confirmation of an executive authorization for Type 2 surveillance issued / the renewal of an executive authorization for Type 2 surveillance granted upon oral application (section 27(1)(a) and (5)(a))

COP-18 Refusal of application for confirmation of an executive authorization for Type 2 surveillance issued / the renewal of an executive authorization for Type 2 surveillance granted upon oral application (section 27(1)(b) and (5)(b))

Report on the discontinuance of Type 2 surveillance

COP-19 Report on the discontinuance of Type 2 surveillance carried out under an executive authorization (section 57(3))

Prescribed Forms for submission to/use by Head of Department

Emergency Application – interception / Type 1 surveillance

COP-20 Application for an emergency authorization for interception / Type 1 surveillance (section 20(1))

COP-21 Emergency authorization for interception / Type 1 surveillance (section 21(1)(a))

COP-22 Refusal of application for an emergency authorization for interception / Type 1 surveillance (section 21(1)(b) and (3)(b))

Report on the discontinuance of interception / Type 1 surveillance carried out under an emergency authorization

COP-23 Report on the discontinuance of interception / Type 1 surveillance carried out under an emergency authorization (section 57(3))

COP-1

[PJO No.]

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 8(1))

APPLICATION FOR AN AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

This is an application under section 8(1) of the Interception of Communications and Surveillance Ordinance for the issue of an authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 Surveillance* to be carried out by or on behalf of any of the officers of the **[name of department]** (the Department).

This application is made by **[name, rank and post]** of the Department.

This application is supported by an affidavit / affirmation* of the applicant.

Dated this the day of .

_____

Signature of applicant

* Delete as appropriate.

[PJO No.]
[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 11(1))

APPLICATION FOR RENEWAL OF AN AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

This is an application under section 11(1) of the Interception of Communications and Surveillance Ordinance for the renewal of an authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* to be carried out by or on behalf of any of the officers of the **[name of department]** (the Department).

The authorization for which renewal is sought is **[ICSO No.]** issued by **[name of panel judge]** on the day of (the authorization).

This application is made by **[name, rank and post]** of the Department.

This application is supported by an affidavit / affirmation* of the applicant, a copy of the authorization sought to be renewed and a copy of the/all* affidavit/s* / affirmation/s* that was / were* provided for the purposes of the application for the issue of that authorization / and renewal/s* of that authorization*.

Dated this the day of .

Signature of applicant

* Delete as appropriate.

COP-3
[PJO No.]
[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 23(1))

APPLICATION FOR CONFIRMATION OF AN EMERGENCY AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

This is an application under section 23(1) of the Interception of Communications and Surveillance Ordinance for confirmation of an emergency authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* carried out / to be carried out* by or on behalf of any of the officers of the **[name of department]** (the Department).

The emergency authorization for which confirmation is sought was issued by **[name and title of the head of department]** on the day of at hours (the emergency authorization).

This application is made by **[name, rank and post]** of the Department.

This application is supported by an affidavit / affirmation* of the applicant and a copy of the emergency authorization.

Dated hours of this the day of .

Signature of applicant

* Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 23(1) and Section 28(1))

APPLICATION FOR CONFIRMATION OF AN EMERGENCY AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE* ISSUED UPON ORAL APPLICATION

This is an application under section 23(1) of the Interception of Communications and Surveillance Ordinance for confirmation of an emergency authorization issued upon oral application.

The emergency authorization for which confirmation is sought is an emergency authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* carried out / to be carried out* by or on behalf of any of the officers of the **[name of department]** (the Department). This emergency authorization was issued by **[name and title of the head of department]** of the Department on the day of at hours.

This application is made by **[name, rank and post]** of the Department.

This application is supported by:

(i) an affidavit / affirmation* of the applicant; and

(ii) a record in writing:

(a) containing all the information that would have been provided under the relevant written application provision had the oral application been made in writing; and

(b) setting out the determination that was orally delivered in respect of that oral application.

Dated hours of this the day of .

Signature of applicant

* Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 26(1))

APPLICATION FOR CONFIRMATION OF AN AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE ISSUED / THE RENEWAL OF AN AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE GRANTED* UPON ORAL APPLICATION

This is an application under section 26(1) of the Interception of Communications and Surveillance Ordinance for confirmation of an authorization issued / the renewal of an authorization granted* upon oral application.

The authorization / renewal of the authorization* for which confirmation is sought is an authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* carried out / to be carried out* by or on behalf of any of the officers of the **[name of department]** (the Department). This is an authorization that was issued / whose renewal was granted* by **[name of panel judge]** on the day of at hours.

This application is made by **[name, rank and post]** of the Department.

This application is supported by:

(i) an affidavit / affirmation* of the applicant; and

(ii) a record in writing:

(a) containing all the information that would have been provided under the relevant written application provision had the oral application been made in writing; and

(b) setting out the determination that was orally delivered in respect of that oral application.

Dated hours of this the day of .

Signature of applicant

* Delete as appropriate.

[PJO No.]
[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 33(1))

APPLICATION FOR A DEVICE RETRIEVAL WARRANT

This is an application under section 33(1) of the Interception of Communications and Surveillance Ordinance for the issue of a device retrieval warrant.

The application is made in respect of a device/devices* authorized to be used under and installed pursuant to a prescribed authorization issued by **[name of panel judge]** on the day of and numbered **[ICSO No.]**.

This application is made by **[name, rank and post]** of **[name of department]**.

This application is supported by an affidavit / affirmation* of the applicant and a copy of the prescribed authorization.

Dated this the day of .

Signature of applicant

* Delete as appropriate.

COP-7

[PJO No.]

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 57(3))

REPORT ON THE DISCONTINUANCE OF INTERCEPTION / TYPE 1 SURVEILLANCE* CARRIED OUT UNDER A PRESCRIBED AUTHORIZATION

This is a report under section 57(3) of the Interception of Communications and Surveillance Ordinance on the discontinuance of interception of communication transmitted by a postal service / a telecommunications system / Type 1 surveillance* under a prescribed authorization.

[I. If the interception / Type 1 surveillance has been carried out]

The prescribed authorization, **[ICSO No.]**, under which the discontinued interception of communication transmitted by a postal service / a telecommunications system / Type 1 surveillance* was carried out by or on behalf of any of the officers of the **[name of department]**, was issued/renewed* by **[name of panel judge]** on the day of .

[I(1) For discontinuance after the decision to discontinue the operation was made]

(A) Single schedule / surveillance

The interception / Type 1 surveillance* was discontinued on the day of at hours, after the decision to discontinue the operation was made by **[name, rank and post of the officer]**, on the day of at hours on the ground that the conditions for the continuance of the prescribed authorization were not met.

(B) Multiple schedules of an interception

The interception of the telecommunications service(s) specified in Schedules(s) [ ] was discontinued on the day of at hours [and hours respectively], after the decision to discontinue the interception was made by **[name, rank and post of the officer]**, on the day of at

---

* Delete as appropriate.

hours on the ground that the conditions for the continuance of the prescribed authorization were not met.

[I(2) For discontinuance before the decision to discontinue the operation was made]

The interception / Type 1 surveillance* was discontinued on the day of at hours, before the decision to discontinue the operation was made by **[name, rank and post of the officer]** on the day of at hours on the ground that the conditions for the continuance of the prescribed authorization were not met.

[I(3) For discontinuance at the same time when the decision to discontinue the operation was made]

The interception / Type 1 surveillance* was discontinued on the day of at hours, at the same time when the decision to discontinue the operation was made by **[name, rank and post of the officer]** on the day of at hours, on the ground that the conditions for the continuance of the prescribed authorization were not met.

[II. If the interception / Type 1 surveillance has not started]

The prescribed authorization, **[ICSO No.]**, was issued/renewed* by **[name of panel judge]** on the day of . The decision not to start the *interception/ Type 1 surveillance was made by **[name, rank and post of the officer]**, on the day of at hours, on the ground that the conditions for the continuance of the prescribed authorization were not met.

The ground for discontinuance described in paragraph I(1)(A) / I(1)(B) / I(2) / I(3) / II* above is as follows:

[Set out details of how the conditions for its continuance were not met]

This report is made by **[name, rank and post]** of the **[name of department]**.

Dated hours of this the day of .

Signature of reporting officer

COP-8

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 14(1))

APPLICATION FOR AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

This is an application under section 14(1) of the Interception of Communications and Surveillance Ordinance for the issue of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the **[name of department]** (the Department).

This application is made by [**name, rank and post]** of the Department for the determination by **[name, rank and post]**, an authorizing officer of the Department.

This application is supported by a statement in writing of the applicant [and a supplementary information sheet]* which is/are annexed to this application.

Dated hours of this the day of .

_____

Signature of applicant

* Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE ORDINANCE

(Section 14(2))

STATEMENT IN WRITING IN SUPPORT OF AN APPLICATION
FOR AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

This is the statement in writing of **[insert name, rank and post]** of the **[name of Department]** (the Department) in support of an application under section 14(1) of the Interception of Communications and Surveillance Ordinance (ICSO) for the issue of an executive authorization for Type 2 surveillance.

Please choose and provide details where appropriate.

1. The Investigation

(a) File No.:

(b) Brief facts of the case:

2. The Section 3 ICSO Purpose for the Issue of the Executive Authorization

(a) The purpose of the Type 2 surveillance is for:

☒ preventing or detecting serious crime

☒ protecting public security

(b) Particulars of the nature of the serious crime or the threat to public security as mentioned in (a) above are:

☒ alleged offence(s), please specify:

maximum penalty, please specify:

☒ threat to public security, please specify:

(c) The grounds for the reasonable suspicion that any person has been, is, or is likely to be, involved in the specific crime or any activity constituting the particular threat to security as referred to in (b) above:

3. The Type 2 Surveillance for Which Executive Authorization is Sought

(i) Particulars of the Type 2 Surveillance

(a) The form of the Type 2 surveillance:
(including the kind(s) of any devices to be used)

(b) If known, whether, during the preceding 2 years, there has been any application for authorization or renewal in which any persons set out in paragraph (iii)(a) below has been identified as the subject of the interception or covert surveillance concerned:
(If positive, state the date of approval or refusal of the previous application and the covered period.)

(c) The proposed duration of the Type 2 surveillance:
(no more than 3 months)
Starting Date: Time:
Finishing Date: Time:

(ii) Particulars of Where the Type 2 Surveillance is to be Carried Out

If known, particulars of any premises, including any land or building, conveyance, structure (whether movable or offshore), object or class of objects in or on which the Type 2 surveillance is to be carried out (i.e. the location at which the surveillance is used/targeted):

(iii) Particulars of Persons Subject To or Affected By the Type 2 Surveillance

(a) The identity of the subject(s) on whom the Type 2 surveillance is to be carried out, if known:

Name (Eng): Name (Chn):
HKIC No./Travel Doc. Type No.:
Address:

OR

If the identity of the person is not known, the description of any such person or class of persons:

(b) The identity of any person other than the subject of the Type 2 surveillance who may be affected by it:

Name (Eng): Name (Chn):
HKIC No./Travel Doc. Type No.:
Address:

OR

If the identity of the person is not known, the description of any such person or class of persons:

(iv) Particulars of the Information Sought to be Obtained by the Type 2 Surveillance

(Note: Examples of the information sought might be the identification of particular persons, such as victims, witnesses, suspects, associates, accomplices, etc.; the identification of particular locations, such as residence, safe houses, haunts, victim's locations, scenes of crime, etc.; and information in relation to particular criminal activities such as criminal act, conspiracy, intended action or motivation suspected to be, about to be or to have been taking place. When describing the information sought, you should relate it back to the investigation so that its relevance to the investigation is apparent.)

The information sought to be obtained from the Type 2 surveillance is:

4. The Section 3 ICSO Proportionality Test

(i) Relevant Factor (a): Immediacy and Gravity of the Crime or Threat

The immediacy and gravity of the serious crime or threat to public security is assessed as follows:

(Note: In the case of a threat to public security, please also provide an assessment of its impact, both direct and indirect, on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong.)

(ii) Relevant Factor (b): Value and Relevance of the Information

The information likely to be obtained by carrying out the Type 2 surveillance is that described in paragraph 3(iv) herein.

(a) The likely value and relevance of the information likely to be obtained is[1]:

(b) The benefits likely to be obtained by carrying out the Type 2 surveillance are:

(Note : Examples of the benefits likely to be obtained might be enabling the investigation to progress; acquiring information or evidence not likely to be acquired by other means;

[1] Describe how, in the circumstances of this specific investigation, the information is likely to be of value and relevant.

enabling the case, the nature of which is grave and, where applicable, needs to be dealt with immediately, to be investigated more speedily; enabling the conduct to be investigated with less risk of harm to officers.)

(iii) The Intrusiveness of the Type 2 Surveillance on Any Person

(a) The intrusiveness of the Type 2 surveillance on any person who is to be the subject of the Type 2 surveillance is as follows[2]:

(b) Assessment of the impact (if any) on persons not being the subject of the Type 2 surveillance but who may be affected by it:
(Note: In addition to assessing the impact, please also describe what the impact will be and any means that could be employed to minimize such impact.)

(c) The likelihood that information which may be subject to legal professional privilege will be obtained:

Whether the office or residence of a lawyer, or other premises ordinarily used by the lawyer and other lawyers for the purpose of provision of legal advice to clients, will be involved in the operation:
[Multi-line text with formatting]

(d) The likelihood that the content of any journalistic material will be obtained:
(Note: Explain also why such likelihood exists and what measures will be taken to minimize the likelihood of it occurring.)

(iv) Whether the Purpose Sought to be Furthered Can Reasonably be Furthered by Other Less Intrusive Means?

(a) Are other less intrusive means of investigation available that could achieve the same result as the Type 2 surveillance?
☐ Yes ☐ No

(b) If "Yes" to (a) above, have such other less intrusive means of investigation been attempted?
☐ Yes ☐ No

(c) If "No" to (b) above, the reason for not using the other less intrusive means of investigation:
(Note: Explain why in the circumstances such less intrusive means of investigation cannot

[2] Describe the type of impact of the Type 2 surveillance on the subject and any means that could be used to minimize it.

reasonably further the purpose sought to be furthered.)

(d) What consequences are likely should the Type 2 surveillance not be authorized?

(Note: The consequences might be that the specific law enforcement investigation or operation could be compromised or the safety of the investigating officers or the public could be endangered. Please ensure that you explain why such consequences are likely to occur should the Type 2 surveillance not be authorized.)

(v) Other matters that are relevant in the circumstances

(a) The proposed duration of the authorization

The proposed duration of the authorization is only for as long as is assessed to be necessary to achieve the purpose set out in paragraph 2 herein and to obtain the information particularized in paragraph 3(iv) herein. The duration sought in paragraph 3(i)(c) herein has been assessed taking into account the following matters:

(b) Any other matters

5. Applicant's Declaration

The information provided above is true to the best of my knowledge and belief and I provide it knowing that if I wilfully state anything which I know to be false or do not believe to be true, I may be liable to prosecution for a criminal offence.

Dated hours of this the day of .

_____

Signature of applicant

Name:	_____	Office Tel.:	_____
Rank:	_____	Mobile.:	_____
Post:	_____	Pager.:	_____
Date:	_____		

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 15(1)(a))

EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

An application under section 14(1) of the Interception of Communications and Surveillance Ordinance (the Ordinance) has been made to me, an authorizing officer of the **[name of Department]** (the Department), for the issue of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the Department.

In support of the application is a statement in writing of the applicant [and a supplementary information sheet]*. On the basis of the information contained in that statement in writing [and the supplementary information sheet]* I am satisfied that the conditions in section 3 of the Ordinance have been met.

I therefore issue this executive authorization for the following Type 2 surveillance to be carried out:

[Insert details of the Type 2 surveillance]

Upon the condition that:
The applicant or any other authorized officer of the Department shall, as soon as practicable, in any event during the validity of this authorization (or any period of renewal thereof) bring to the attention of an authorizing officer of the Department any:
(i) initial material inaccuracies, or
(ii) material change of circumstances,
upon which this authorization is granted (or later renewed) which the applicant becomes aware of during such period of validity or renewal.

This executive authorization takes effect from the day of at hours and remains in force **[please specify a period which should in no case be longer than 3 months from the time when the executive authorization takes effect]**.

Issued at hours of this the day of .

_____

Signature of authorizing officer
[Name/rank/post of authorizing officer]

_____

*Delete as appropriate.

COP-11

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 15(1)(b) and (3)(b))

REFUSAL OF APPLICATION FOR AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

An application under section 14(1) of the Interception of Communications and Surveillance Ordinance has been made to me, an authorizing officer of the **[name of department]** (the Department), for the issue of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the Department.

In support of the application is a statement in writing of the applicant [and a supplementary information sheet]*. I hereby refuse the application for the following reasons:

Dated this the day of .

_____

Signature of authorizing officer

[Name / rank / post of authorizing officer]

*Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 17(1))

APPLICATION FOR RENEWAL OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

This is an application under section 17(1) of the Interception of Communications and Surveillance Ordinance for the renewal of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the **[name of department]** (the Department).

The executive authorization for which renewal is sought is **[ICSO No.]** and was issued by **[name, rank and post of the authorizing officer]** on the day of .

This application is made by **[name, rank and post]** of the Department for the determination by **[name, rank and post]**, an authorizing officer of the Department.

This application is supported by a statement in writing of the applicant, [a supplementary information sheet],* a copy of the executive authorization sought to be renewed and a copy of a/all statement/s* in writing [and supplementary information sheet/s]* that was/were* provided for the purposes of the application for the issue of that executive authorization/and renewal/s* of that executive authorization.

Dated hours of this the day of .

_____

Signature of applicant

* Delete as appropriate

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE ORDINANCE

(Section 17(2))

STATEMENT IN WRITING IN SUPPORT OF AN APPLICATION
FOR RENEWAL OF AN EXECUTIVE AUTHORIZATION
FOR TYPE 2 SURVEILLANCE

This is the statement in writing of **[name, rank and post]** of the **[name of department]** (the Department) in support of an application under section 17(1) of the Interception of Communications and Surveillance Ordinance (ICSO) for the renewal of an executive authorization for Type 2 surveillance.

Please choose and provide details where appropriate.

1. The Previous Investigation

(a) File No.:

(b) Details of an assessment of the value of information so far obtained pursuant to the executive authorization/and its previous renewal/s*:

2. The Renewal Application

(a) No. of renewal application(s) sought previously:
(List each occasion, as well as date(s) of approval and the duration covered)

* Delete as appropriate

(b) Reason for the renewal
(include the expiry date and time of the existing executive authorization and the consequence of not renewing the authorization)

(c) Details of any significant change to the information previously provided for the application for the authorization or renewal

(d) The proposed duration of the renewal:
(no more than 3 months)
Starting Date*: Time*:
* In accordance with section 19(a) of the ICSO, the renewal should take effect at the time when the executive authorization would have ceased to take effect but for the renewal.
Finishing Date: Time:

The proposed duration of the renewal sought above is assessed as being necessary to achieve the purpose of the executive authorization, taking into account the following matters:

(e) The identity of any person other than the subject of the Type 2 surveillance who has not been mentioned in the previous application for the executive authorization or its renewal and who may be affected by it:

Name (Eng): Name (Chn):
HKIC No./Travel Doc. Type No.:
Address:

OR

If the identity of the person is not known, the description of any such person or class of persons:

(f) The intrusiveness of the Type 2 Surveillance on any person other than the subject

(i) Assessment of the impact (if any) on persons not being the subject of the Type 2 surveillance but who may be affected by it:
(Note: In addition to assessing the impact, please also describe what the impact will be and any means that could be employed to minimize such impact.)

(ii) The likelihood that information which may be subject to legal professional privilege will be obtained :

Whether the office or residence of a lawyer, or other premises ordinarily used by the lawyer and other lawyers for the purpose of provision of legal advice to clients, will be involved in the operation:

(iii) The likelihood that the content of any journalistic material will be obtained:
(Note: Explain also why such likelihood exists and what measures will be taken to minimize the likelihood of it occurring.)

3. Applicant's Declaration

The information provided above is true to the best of my knowledge and belief and I provide it knowing that if I wilfully state anything which I know to be false or do not believe to be true, I may be liable to prosecution for a criminal offence.

Dated hours of this the day of .

_____
Signature of applicant

Name: _____ Office Tel.: _____
Rank: _____ Mobile: _____
Post: _____ Pager: _____
Date: _____

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 18(1)(a) and (3)(a))

RENEWED EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

An application under section 17(1) of the Interception of Communications and Surveillance Ordinance (the Ordinance) has been made to me, an authorizing officer of the **[name of department]** (the Department), for the renewal of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the Department.

The executive authorization for which renewal is sought is **[ICSO No.]** issued by **[name, rank and post of authorizing officer]** on the day of (the executive authorization).

In support of the application is a statement in writing of the applicant, [a supplementary information sheet,]* a copy of the executive authorization sought to be renewed and a copy of the/all* statement/s* in writing [and supplementary information sheet/s*] that was/were* provided for the purposes of the application for the issue of that executive authorization / and renewal/s* of that executive authorization*. On the basis of the information contained in these documents I am satisfied that the conditions in section 3 of the Ordinance have been met.

I therefore grant the renewal sought under the application for the following Type 2 surveillance to be carried out:

[Insert details of the Type 2 surveillance]

Upon the condition that:
The applicant or any other authorized officer of the Department shall, as soon as practicable, in any event during the validity of this authorization (or any period of renewal thereof) bring to the attention of an authorizing officer of the Department any:
(i) initial material inaccuracies, or
(ii) material change of circumstances,
upon which this authorization is granted (or later renewed) which the applicant becomes aware of during such period of validity or renewal.

This renewed executive authorization takes effect from the day of at hours and remains in force **[please specify a period which should in no case be longer than 3 months from the time when the renewed executive authorization takes effect]**.

Issued at hours of this the day of .

_____

Signature of authorizing officer
[Name/rank/post of authorizing officer]

*Delete as appropriate

COP-15

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE ORDINANCE

(Section 18(1)(b) and (3)(b))

REFUSAL OF APPLICATION FOR RENEWAL OF
AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

An application under section 17(1) of the Interception of Communications and Surveillance Ordinance has been made to me, an authorizing officer of the **[insert name of department]** (the Department), for the renewal of an executive authorization for Type 2 surveillance to be carried out by or on behalf of any of the officers of the ICAC.

The executive authorization for which renewal is sought is **[ICSO No.]** issued by **[name, rank and post of authorizing officer]** on the day of (the executive authorization).

In support of the application is a statement in writing of the applicant, [a supplementary information sheet],* a copy of the executive authorization sought to be renewed and a copy of the/all statement/(s)* in writing [and supplementary information sheet/(s)]* that was/were* provided for the purposes of the application for the issue of that executive authorization/ and renewal/s* of that executive authorization*.

I hereby refuse to grant the renewal for the following reasons:

Dated this the day of .

_____

Signature of authorizing officer
[Name / rank / post of authorizing officer]

* Delete as appropriate.

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 26(1))

APPLICATION FOR CONFIRMATION OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE ISSUED / THE RENEWAL OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE GRANTED* UPON ORAL APPLICATION

This is an application under section 26(1) of the Interception of Communications and Surveillance Ordinance for confirmation of an executive authorization issued / the renewal of an executive authorization granted* upon oral application.

The executive authorization / renewal of the executive authorization* for which confirmation is sought is an executive authorization for Type 2 surveillance carried out / to be carried out* by or on behalf of any of the officers of the **[name of department]** (the Department). This is an executive authorization that was issued / whose renewal was granted* by **[name, rank and post of the authorizing officer]** on the day of at hours.

This application is made by **[name, rank and post]** of the Department for the determination by **[name, rank and post]**, an authorizing officer of the Department.

This application is supported by the following documents which are annexed to this application:

(i) a statement in writing of the applicant; and

(ii) a record in writing:

(a) containing all the information that would have been provided under the relevant written application provision had the oral application been made in writing; and

(b) setting out the determination that was orally delivered in respect of that oral application.

---

* Delete as appropriate

Dated hours of this the day of .

Signature of applicant

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 27(1)(a) and (5)(a))

CONFIRMATION OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE ISSUED/ THE RENEWAL OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE GRANTED* UPON ORAL APPLICATION

An application under section 26(1) of the Interception of Communications and Surveillance Ordinance (the Ordinance) has been made to me, an authorizing officer of the **[name of department]** (the Department), for confirmation of an executive authorization issued/ the renewal of an executive authorization granted* upon oral application.

The executive authorization/ renewal of the executive authorization* for which confirmation is sought is an executive authorization for Type 2 surveillance carried out/ to be carried out* by or on behalf of any of the officers of the Department. This executive authorization was issued/ The renewal of this executive authorization was granted* by me / **[name, rank and post of the authorizing officer]*** on the day of at hours, to be valid between hours on day of and hours on day of , in the following terms:

[Insert details of the Type 2 surveillance.]

Upon the condition that:
The applicant or any other authorized officer of the Department shall, as soon as practicable, in any event during the validity of this authorization (or any period of renewal thereof) bring to the attention of an authorizing officer of the Department any:
(i) initial material inaccuracies, or
(ii) material change of circumstances,
upon which this authorization is granted (or later renewed) which the applicant becomes aware of during such period of validity or renewal.

This application for confirmation is supported by:
(i) a statement in writing of the applicant; and
(ii) a record in writing:
(a) containing all the information that would have been provided under the relevant written application provision had the oral application

been made in writing; and

(b) setting out the determination that was orally delivered in respect of that oral application.

On the basis of the information contained in these documents, I am satisfied that the conditions in section 3 of the Ordinance have been met in the issue/renewal* of the executive authorization.

I hereby confirm the abovementioned executive authorization / renewal of the executive authorization* and this is issued accordingly.

Dated hours of this the day of .

_____

Signature of authorizing officer

[Name/rank/post of authorizing officer]

_____

*Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 27(1)(b) and (5)(b))

REFUSAL OF APPLICATION FOR CONFIRMATION OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE ISSUED / THE RENEWAL OF AN EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE GRANTED* UPON ORAL APPLICATION

An application under section 26(1) of the Interception of Communications and Surveillance Ordinance (the Ordinance) has been made to me, an authorizing officer of the **[name of department]** (the Department), for confirmation of an executive authorization issued / the renewal of an executive authorization granted* upon oral application.

The executive authorization / renewal of the executive authorization* for which confirmation is sought is an executive authorization for Type 2 surveillance carried out / to be carried out* by or on behalf of any of the officers of the Department. This executive authorization was issued / The renewal of this executive authorization was granted* by **[name, rank and post of the authorizing officer]** on the day of at hours.

This application is supported by:

(i) a statement in writing of the applicant; and

(ii) a record in writing:

(a) containing all the information that would have been provided under the relevant written application provision had the oral application been made in writing; and

(b) setting out the determination that was orally delivered in respect of that oral application.

I hereby refuse to confirm the authorization / renewal* for the following reasons:

---

* Delete as appropriate

In accordance with the provisions of section 27(5)(b), I make the following orders under section 27(3) of the Ordinance:

(i) the executive authorization / renewal* is revoked upon the making of this determination refusing the confirmation / is only to have effect subject to the following variations from the time of this determination*:

(ii) the immediate destruction of the information obtained by carrying out the Type 2 surveillance as specified below: *(Note: In case of revocation, this must include all information obtained by the Type 2 surveillance.)*

Dated hours of this the day of .

Signature of authorizing officer
[Name / rank / post of authorizing officer]

* Delete as appropriate

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 57(3))

REPORT ON THE DISCONTINUANCE OF TYPE 2 SURVEILLANCE CARRIED OUT UNDER AN EXECUTIVE AUTHORIZATION

To: **[insert name, rank and post of the authorizing officer]** of the **[name of the Department]** (the Department)

This is a report under section 57(3) of the Interception of Communications and Surveillance Ordinance on the discontinuance of Type 2 surveillance under an executive authorization.

[If the Type 2 surveillance has been carried out]
The executive authorization, **[ICSO No.]**, under which the discontinued Type 2 surveillance was carried out by or on behalf of any of the officers of the Department, was issued/renewed* by you / **[name, rank and post of the authorizing officer]*** on the day of .

The Type 2 surveillance was discontinued on the day of at hours, before/ after/ at the same time when* the decision to discontinue the operation was made by **[name, rank and post of the officer]**, on the day of at hours on the ground that the conditions for the continuance of the prescribed authorization were not met.

[Set out details of how the conditions for its continuance were not met]

[If the Type 2 surveillance has not started]

The executive authorization, [ICSO No.], was issued/renewed* by you / **[name, rank and post of the authorizing officer]*** on the day of . The decision to discontinue the operation was made by **[name, rank and post of the officer],** on the day of at hours, prior to the Type 2 surveillance being carried out under the executive authorization, on the ground that the conditions for the continuance of the prescribed authorization were not met.

[Set out details of how the conditions for its continuance were not met]

This report is made by **[name, rank and post]** of the Department.

Dated hours of this the day of .

_____
Signature of reporting officer

_____
*Delete as appropriate.

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE ORDINANCE

(Section 20(1))

APPLICATION FOR AN EMERGENCY AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

This is an application under section 20(1) of the Interception of Communications and Surveillance Ordinance for an emergency authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* to be carried out by or on behalf of any of the officers of the **[name of department]** (the Department).

This application is made by **[name, rank and post]** for the determination by **[name and title of the head of department]**.

This application is supported by a statement in writing of the applicant which is annexed to this application.

Dated hours of this the day of .

Signature of applicant

* Delete as appropriate

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 21(1)(a))

EMERGENCY AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

An application under section 20(1) of the Interception of Communications and Surveillance Ordinance (the Ordinance) has been made to me, the Head of the **[name of department]** (the Department), for the issue of an emergency authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* to be carried out by or on behalf of any of the officers of the Department.

In support of the application is a statement in writing of the applicant. On the basis of the information contained in that statement in writing I am satisfied that (1) the circumstances of an emergency authorization as set out in section 20(1)(a) and (b) applied; and (2) the conditions for the issue of the emergency authorization under section 3 of the Ordinance have been met.

I therefore issue this emergency authorization for the following interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* to be carried out:

> **[Insert details of the interception or Type 1 surveillance and any variations and any conditions imposed under section 32, in addition to those stated below]**

The emergency authorization is subject to the following conditions:

The applicant or any other authorized officer of the Department shall, as soon as practicable, and in any event during the validity of this emergency authorization, bring to the attention of the head of department as well as any Panel Judge any:

(i) initial material inaccuracies; or
(ii) material change of circumstances upon which this emergency authorization is granted,

which the applicant becomes aware of during such period of validity.

---

* Delete as appropriate

This emergency authorization takes effect from the day of at hours and remains in force **[please specify a period which should in no case be longer than 48 hours from the time the emergency authorization is issued]**.

Dated hours of this the day of .

_____

Signature of head of department

[Name / title of the head of department]

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE

(Section 21(1)(b) and (3)(b))

REFUSAL OF APPLICATION FOR AN EMERGENCY AUTHORIZATION FOR INTERCEPTION / TYPE 1 SURVEILLANCE*

An application under section 20(1) of the Interception of Communications and Surveillance Ordinance has been made to me, the Head of the **[name of department]** (the Department), for the issue of an emergency authorization for the interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* to be carried out by or on behalf of any of the officers of the Department.

In support of the application is a statement in writing of the applicant. I hereby refuse the application for the following reasons:

Dated hours of this the day of .

Signature of head of department
[Name / title of the head of department]

* Delete as appropriate

[ICSO No.]

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE ORDINANCE

(Section 57(3))

REPORT ON THE DISCONTINUANCE
OF INTERCEPTION / TYPE 1 SURVEILLANCE*
CARRIED OUT UNDER AN EMERGENCY AUTHORIZATION

To: **[insert name and title of the head of department]** of the **[name of the Department] (the Department)**

This is a report under section 57(3) of the Interception of Communications and Surveillance Ordinance on the discontinuance of interception / Type 1 surveillance* under an emergency authorization.

[If the interception / Type 1 surveillance has been carried out]

The emergency authorization, **[ICSO No.]**, under which the discontinued interception of a communication transmitted by post / a telecommunications system / Type 1 surveillance* was carried out by or on behalf of any of the officers of the Department, was issued by you / **[name and title of head of department]*** on the day of at hours.

The interception / Type 1 surveillance was discontinued on the day of at hours after the decision to discontinue the operation was made by the officer-in-charge, **[name, rank and post of the officer]**, on the day of at hours on the ground that the conditions for the continuance of the prescribed authorization were not met.

[Set out details of how the conditions for its continuance were not met]

[If the interception / Type 1 surveillance has not started]

The emergency authorization, **[ICSO No.]**, was issued by you / **[name and title of head of department]** on the day of at hours. The decision to discontinue the operation was made by the officer-in-charge, **[name, rank and post of the officer]**, on the day of at hours, prior to the interception / Type 1 surveillance* being carried out under the prescribed

* Delete as appropriate

authorization, on the ground that the conditions for the continuance of the prescribed authorization were not met.

[Set out details of how the conditions for its continuance were not met]

This report is made by **[name, rank and post]** of the Department.

Dated hours of this the day of .

Signature of reporting officer