

Annual Report 2019 to the Chief Executive

by

The Commissioner on
Interception of Communications
and Surveillance

June 2020

截取通訊及監察事務專員辦公室

Office of the Commissioner on Interception of Communications and Surveillance

本處檔號 Our ref.: ICS/12/1C Pt.6

電話 Tel. No.:

來函檔號 Your ref.:

傳真 Fax No.:

29 June 2020

The Honourable Mrs Carrie Lam Cheng Yuet-ngor, GBM, GBS
The Chief Executive
Hong Kong Special Administrative Region
People's Republic of China

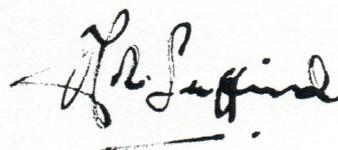
CONFIDENTIAL

Dear Madam,

Annual Report for the Year 2019

I have the pleasure, pursuant to section 49 of the Interception of Communications and Surveillance Ordinance, in submitting to you the annual report for the year 2019, together with its Chinese translation.

Yours sincerely,



(A. R. Suffiad)

Commissioner on Interception of
Communications and Surveillance

Encl: Annual Report for 2019

CONTENTS

<i>Chapter</i>		Page
	<i>Abbreviations</i>	<i>iv – vi</i>
1	Introduction	1 – 4
2	Interception	5 – 15
3	Covert Surveillance	16 – 29
4	Legal Professional Privilege and Journalistic Material	30 – 38
5	Application for Examination and Notification to Relevant Person	39 – 44
6	Non-compliance, Irregularities and Incidents	45 – 72
7	Recommendations to Heads of Law Enforcement Agencies	73 – 74
8	Statutory Tables	75 – 131
9	Review of Compliance by Law Enforcement Agencies	132 – 137
10	Acknowledgement and Way Forward	138 – 139

<i>Tables in Chapter 8</i>		Page
Table 1(a)	- interception - number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)]	78
Table 1(b)	- surveillance - number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)]	79
Table 2(a)	- interception - major categories of offences for the investigation of which prescribed authorizations have been issued or renewed [section 49(2)(b)(i)]	80
Table 2(b)	- surveillance - major categories of offences for the investigation of which prescribed authorizations have been issued or renewed [section 49(2)(b)(i)]	81
Table 3(a)	- interception - number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]	82
Table 3(b)	- surveillance - number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]	82
Table 4	- interception and surveillance - number of device retrieval warrants issued and number of applications for the issue of device retrieval warrants refused [section 49(2)(c)(i) and (ii)]	83

<i>Tables in Chapter 8</i>		Page
Table 5	– summary of reviews conducted by the Commissioner under section 41 [section 49(2)(d)(i)]	84 – 117
Table 6	– number and broad nature of cases of irregularities or errors identified in the reviews [section 49(2)(d)(ii)]	118 – 122
Table 7	– number of applications for examination that have been received by the Commissioner [section 49(2)(d)(iii)]	123
Table 8	– respective numbers of notices given by the Commissioner under section 44(2) and section 44(5) further to examinations [section 49(2)(d)(iv)]	123
Table 9	– number of cases in which a notice has been given by the Commissioner under section 48 [section 49(2)(d)(v)]	124
Table 10	– broad nature of recommendations made by the Commissioner under sections 50, 51 and 52 [section 49(2)(d)(vi)]	125 – 126
Table 11	– number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or surveillance carried out pursuant to a prescribed authorization [section 49(2)(d)(vii)]	127
Table 12	– number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 42, 47, 52 or 54 and the broad nature of such action [section 49(2)(d)(viii)]	128 – 131

Abbreviations

Unless the context otherwise requires:

affidavit/affirmation/ statement	affidavit or affirmation in support of an application to a panel judge for a prescribed authorization/statement in writing in support of an application to an authorizing officer for an executive authorization
ATR	audit trail report
Cap.	chapter in the Laws of Hong Kong
capable device	device capable of being used for covert surveillance
Code of Practice, COP	the Code of Practice issued by the Secretary for Security under section 63 of the Ordinance
Commissioner	Commissioner on Interception of Communications and Surveillance
CSP	communications services provider
discontinuance report	report on discontinuance of interception or covert surveillance submitted pursuant to section 57 of the Ordinance
DMS	device management system
fresh application	application for a prescribed authorization which is not a renewal
ICSO, Ordinance	Interception of Communications and Surveillance Ordinance (Cap. 589)
interception	interception of communications

JM	journalistic material
LEA	a law enforcement agency under the Ordinance, namely, Customs and Excise Department, Hong Kong Police Force, Immigration Department or Independent Commission Against Corruption
LPP	legal professional privilege
LPP information	information protected by legal professional privilege
non-ICSO purpose	purpose which is not related to ICSO
panel judge	a panel judge appointed under section 6 of the Ordinance
PJO	Panel Judges' Office
QR Code	Quick Response Code
renewal application	application for renewal of a prescribed authorization
RSM	removable storage media
REP-1 report	report on arrest of subject of interception or covert surveillance made on form REP-1
REP-11 report/ REP-13 report	report on material change in circumstances or initial material inaccuracies under a prescribed authorization made on form REP- 11 or form REP-13

Reported LPP Call	a call with LPP likelihood, heightened LPP likelihood or LPP information and is reported to the panel judge by way of an REP-11 report on such
Secretariat	Secretariat, Commissioner on Interception of Communications and Surveillance
section	section of the Ordinance
statutory activity	interception of communications and/or covert surveillance activity referred to in the Ordinance
the report period	the period from 1 January to 31 December 2019
the Team	a dedicated team comprising officers from the LEAs that operates independently of their investigative arms
weekly report form	the form designed for the LEAs and the PJO to provide information to the Commissioner once every week

CHAPTER 1

INTRODUCTION

1.1 Pursuant to section 49 of the Interception of Communications and Surveillance Ordinance (Cap. 589) ('Ordinance' or 'ICSO'), the Commissioner on Interception of Communications and Surveillance ('Commissioner') is required to submit to the Chief Executive an annual report ending on 31 December in each year. This report covers the period 1 January to 31 December 2019.

1.2 The ICSO came into operation in August 2006 and was amended with the enactment of the Interception of Communications and Surveillance (Amendment) Ordinance 2016 in June 2016. The ICSO provides a statutory regime to regulate the conduct of interception of communications, through the post or through the use of telecommunications facilities, and covert surveillance by the use of surveillance devices (collectively called 'statutory activities') by public officers of the four law enforcement agencies ('LEAs'), namely, Customs and Excise Department, Hong Kong Police Force, Immigration Department and Independent Commission Against Corruption. The regulation is to ensure that these statutory activities cannot be lawfully and properly carried out unless the relevant requirements stipulated in the Ordinance are satisfied.

1.3 The first and foremost of the relevant requirements is that any statutory activity can only be lawfully and properly conducted by an officer of an LEA pursuant to a prescribed authorization granted by a relevant authority. The relevant authority includes a panel judge who is empowered to issue a prescribed authorization for interception or for Type 1 surveillance and an authorizing officer of the LEA concerned who can issue a prescribed authorization for Type 2 surveillance. After

obtaining a prescribed authorization, the LEA and its officers are required to comply with its terms in carrying out the statutory activity so authorized. They are also required to observe the provisions of the Code of Practice ('COP') issued by the Secretary for Security under section 63 of the ICSO and other relevant requirements.

1.4 Whether a prescribed authorization should be granted is expressly based on the necessity and proportionality principles, and the premise that the well-being of Hong Kong can be achieved by striking a fair and proper balance between the need for the prevention and detection of serious crime and the protection of public security on the one hand and safeguarding the privacy and other rights of persons in Hong Kong on the other.

1.5 An important function of the Commissioner is to oversee the compliance by the LEAs and their officers with the relevant requirements of the scheme of the ICSO. When this function is engaged, the objects and spirit of the Ordinance must be at the forefront of the oversight. Another function of the Commissioner is to make recommendations to the Secretary for Security on the COP and to the LEAs on their arrangements to better carry out the objects of the Ordinance and the provisions of the COP.

1.6 Various ways of checking the compliance of the LEAs with the relevant requirements, including the examination of the protected products, continued to operate smoothly in 2019.

1.7 As an on-going commitment since I assumed the office of the Commissioner, I continue to render my views to the Security Bureau on the arrangements for better operation of the ICSO and make recommendations to the LEAs for tackling existing and anticipated problems in relation to the ICSO. Recommendations on the COP will also be made when the need arises. This engagement is significant for the benefits of the society in respect of protection of privacy and other rights of individuals.

1.8 In January 2019, a forum on the interception of communications and surveillance was held by the Security Bureau for the relevant officers of the four LEAs under the ICSO. At the invitation of the Security Bureau, I delivered two briefing sessions in the forum, one on telecommunications interception and another one on covert surveillance. I shared with the LEAs some non-compliance cases and irregularities mentioned in previous annual reports as well as certain key points to note. I also put particular emphasis on the importance of and suggested measures and guidelines in protecting information subject to legal professional privilege ('LPP') and enlightened the LEAs on scenarios which constituted heightened LPP likelihood. The forum provided a valuable opportunity in refreshing the knowledge and awareness of the LEAs in complying with the requirements of the ICSO and in enhancing their understanding, professional knowledge and sensitivity in conducting the interception and covert surveillance in a proper and lawful way.

1.9 During the periodical visits to the LEAs on checking of files and documents and after the examination of protected products, I noticed that generally the LEAs had taken cautious approaches in conducting covert operation and handling protected products in order to guard against the obtainment of information subject to LPP and journalistic material ('JM'). I kept on reminding the LEAs to stay vigilant on the protection of LPP information or handling of JM. In the report period, there was a slight decrease in the number of reported new cases that were likely to involve LPP information as compared with last year. Details are given in Chapter 4 of this report.

1.10 In this annual report, I have continued the practice of providing the utmost transparency of my work as the Commissioner, while taking care not to divulge any information the disclosure of which may prejudice the prevention or detection of crime or the protection of public security. I must point out that it is crucial not to reveal information that might be useful to individuals who may be involved in criminal activities

in Hong Kong. In this regard, I have included as much information as possible insofar as its publication does not amount to contravention of the non-prejudice principle.

CHAPTER 2

INTERCEPTION

Prescribed authorizations for interception

2.1 Under section 29(1) of the Ordinance, a prescribed authorization for interception may –

- (a) in the case of a postal interception, authorize one or both of the following –
 - (i) the interception of communications made to or from any premises or address specified in the prescribed authorization;
 - (ii) the interception of communications made to or by any person specified in the prescribed authorization (whether by name or by description); or
- (b) in the case of a telecommunications interception, authorize one or both of the following –
 - (i) the interception of communications made to or from any telecommunications service specified in the prescribed authorization;
 - (ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, or is reasonably expected to use.

Written applications

2.2 Applications for the issue or renewal of a prescribed authorization should normally be made in writing to a panel judge unless it is not reasonably practicable to do so. During the report period, there were a total of 1,314 written applications for interception made by the LEAs, of which 1,310 were granted and four were refused by the panel judges. Among the successful applications, 631 were for authorizations for the first time ('fresh applications') and 679 were for renewals of authorizations that had been granted earlier ('renewal applications').

Reasons for refusal

2.3 The four refused applications were fresh applications, which were refused because the materials provided to support the allegations put forth were insufficient.

Emergency authorizations

2.4 An officer of an LEA may apply to the head of his department for the issue of an emergency authorization for any interception if he considers that there is immediate need for the interception to be carried out due to an imminent risk of death or serious bodily harm of any person, substantial damage to property, serious threat to public security or loss of vital evidence, and having regard to all the circumstances of the case that it is not reasonably practicable to apply to a panel judge for the issue of a judge's authorization. An emergency authorization shall not last for more than 48 hours and may not be renewed. As soon as reasonably practicable and in any event within the period of 48 hours from the issue of the emergency authorization, the head of the department shall cause an officer of the department to apply to a panel judge for confirmation of the

emergency authorization where any interception is carried out pursuant to the emergency authorization.

2.5 During the report period, no application for emergency authorization for interception was made by any of the LEAs.

Oral applications

2.6 An application for the issue or renewal of a prescribed authorization may be made orally if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make a written application in accordance with the relevant written application provisions under the Ordinance. The relevant authority may orally deliver his determination to issue the prescribed authorization or give the reasons for refusing the application. The COP issued by the Secretary for Security provides that the oral application procedures should only be resorted to in exceptional circumstances and in time-critical cases where the normal written application procedures cannot be followed. An oral application and the authorization granted as a result of such an application are regarded as having the same effect as a written application and authorization. Similar to emergency authorizations, the head of the department shall cause an officer of the department to apply in writing to the relevant authority for confirmation of the orally granted prescribed authorization as soon as reasonably practicable and in any event within 48 hours from the issue of the authorization, failing which the prescribed authorization is to be regarded as revoked upon the expiration of the 48 hours.

2.7 During the report period, no oral application for interception was made by any of the LEAs.

Duration of authorizations

2.8 For over 84% of the cases (fresh authorizations as well as renewals) granted by the panel judges during the report period, the duration of the prescribed authorizations was for a period of one month or less, short of the maximum of three months allowed by the Ordinance. While the longest approved duration was 37 days, the shortest one was for several days only. Overall, the average duration of all the authorizations was about 30 days. This indicates that the panel judges handled the applications carefully and applied a stringent control over the duration of the authorizations.

Offences

2.9 Table 2(a) in Chapter 8 gives a list of the major categories of offences for the investigation of which prescribed authorizations for interception had been issued or renewed during the report period.

Revocation of authorizations

2.10 Under section 57(1) of the Ordinance, an officer of an LEA, who conducts any regular review pursuant to the arrangements made under section 56 by his head of department, has a responsibility to discontinue an interception or a part of an interception (and also covert surveillance or a part of covert surveillance) if he is of the opinion that a ground for discontinuance of the prescribed authorization or a part of the prescribed authorization exists. A similar obligation also attaches to the officer who is for the time being in charge of the operation after he becomes aware that such a ground exists. The officer concerned shall then report the discontinuance and the ground for discontinuance to the relevant authority who shall revoke the prescribed authorization concerned or the relevant part of the prescribed authorization concerned.

2.11 The number of authorizations for interception revoked fully under section 57 during the report period was 587. Another 23 cases involved the cessation of a part, but not all, of the interception approved under a prescribed authorization, so that while the prescribed authorization was partially revoked, the remaining part of the interception approved continued to be in force.

2.12 The grounds for discontinuance were that the interception operation was not or no longer productive, the subject had been arrested, the subject had stopped using the telecommunications facility concerned for his criminal activities, or the value to continue the interception operation was considered not proportional to the risk of obtaining LPP information, etc.

2.13 Revocation of authorizations is also expressly provided for in section 58 of the Ordinance. Where the relevant authority (a panel judge) receives a report from an LEA that the subject of an interception has been arrested, with an assessment of the effect of the arrest on the likelihood that any LPP information will be obtained by continuing the interception, he shall revoke the prescribed authorization if he considers that the conditions under the Ordinance for the continuance of the prescribed authorization are not met. The arrest of the subject may or may not relate to the offence(s) for which the interception is authorized to investigate, but all the same the officer of the LEA in charge of the interception who has become aware of the arrest is obliged by section 58 to make the report with the assessment to the panel judge. If the conditions for the continuance of the prescribed authorization are still met, the panel judge may decide not to revoke it. During the report period, the LEAs were aware of a total of 138 arrests but only 21 section 58 reports, which should be made through a prescribed form (i.e. REP-1 report), were made to the panel judge. The panel judge allowed the interception operations related to the 21 section 58 reports to continue subject to additional conditions to guard against the risk of obtaining LPP information. As regards the other arrest

cases, decisions were made by the LEAs concerned to discontinue the interception operations pursuant to section 57 instead of resorting to the section 58 procedure. This reflects the fact that the LEAs were appreciative of the risk of obtaining LPP information after an arrest.

2.14 Section 58A of the Ordinance provides that, where the relevant authority (a panel judge) receives a report from an LEA on material change in circumstances or material inaccuracies under a prescribed authorization, he shall revoke the prescribed authorization if he considers that the conditions under the Ordinance for the continuance of the prescribed authorization are not met. During the report period, no authorization for interception was revoked by the panel judge under this section of the Ordinance.

Authorizations with five or more previous renewals

2.15 There were 12 authorizations for interception with five or more previous renewals within the report period. All the cases with six renewals and some of their further renewals were checked and found in order during periodical visits to the LEAs.

Arrests attributable to interception

2.16 It is and continues to be the common view of the LEAs that interception is a very effective and valuable investigation tool in the prevention and detection of serious crime and the protection of public security. It has to be pointed out that under section 61 of the Ordinance, any telecommunications interception product shall not be admissible in evidence in any proceedings before any court other than to prove that a relevant offence has been committed. Therefore, whatever is obtained by way of interception can only be used by way of intelligence. The intelligence gathered from interception very often leads to a fruitful and successful conclusion of an investigation. During the report period, a

total of 120 persons, who were subjects of prescribed authorizations, were arrested as a result of or further to interception operations. In addition, 169 non-subjects were also arrested consequent upon the interception operations.

Procedure of oversight for interception

2.17 The LEAs' compliance with the requirements of the Ordinance in respect of the interception cases reported in 2019 was reviewed by the following ways:

- (a) checking of the weekly reports submitted by the LEAs and the Panel Judges' Office ('PJO');
- (b) examination of the contents of the LEAs' files and documents during periodical visits to the LEAs;
- (c) examination of interception products at the LEAs' offices; and
- (d) counter-checking the facilities intercepted with non-LEA parties such as communications services providers ('CSPs') and through other means.

The following paragraphs further explain how the above reviews were carried out.

Checking of weekly reports

2.18 The LEAs were required to submit weekly reports to the Secretariat on their respective applications, successful or otherwise, and other relevant reports made to the panel judges/departmental authorizing officers by way of completing forms designed for the purpose ('weekly report forms'). Such weekly reports deal with all statutory activities, i.e. interception and covert surveillance. At the same time, the PJO was

also requested to submit weekly report forms on the applications they received from all the LEAs, approved or refused, and the revocations of prescribed authorizations. A weekly report covers the statutory activities with related authorizations and refused applications in the entire week before the week of its submission to the Secretariat.

2.19 The weekly report forms only contain general information relating to cases of the related week such as whether the application was successful or rejected, the duration of the authorization, the offences involved, the assessment on the likelihood of obtaining LPP information and JM from the proposed operation, etc. Case background, progress of the investigation, identity and particulars of the subject and others as well as other sensitive information are not required and therefore obliterated or sanitised so that such information will always be kept confidential with minimal risk of leakage.

2.20 Upon receipt of the weekly report forms from the LEAs, the Secretariat would study the details of each weekly report form and, except those relating to Type 2 surveillance, counter-check against the PJO's returns. In case of discrepancies or doubts, clarification and explanation were sought from the LEAs and/or the PJO as and when necessary.

Examination of documents and information during periodical visits

2.21 Should the Commissioner perceive a need, clarification and explanation on the weekly report forms would also be sought in the periodical visits to the offices of the LEAs. In the visits, the Commissioner would also select, on a random basis, some other cases for examination apart from those requiring clarification. Documents to be scrutinised by the Commissioner would include the originals of the applications, reports on discontinuance, reports on material change in circumstances, reports on material inaccuracies, case files and internal review documents, etc. Such visits were carried out so that secret or sensitive information

contained in case files and documents that would otherwise be required to be sent to the Secretariat for checking would always remain in the safety of the LEAs' offices to avoid any possible leakage.

2.22 If questions or doubts still could not be resolved after the examination of such documents, the Commissioner would require the LEA to answer the queries or to explain the cases in greater detail.

2.23 In addition to matters relating to minor discrepancies in the weekly reports from the LEAs and the PJO, a total of 898 applications for interception, including granted authorizations and refused applications, and 767 related documents/matters had been checked during the Commissioner's periodical visits to the LEAs in the report period.

Examination of interception products

2.24 Having the express power to examine the protected products after the enactment of the Interception of Communications and Surveillance (Amendment) Ordinance 2016, the Commissioner and his delegated officers have carried out the relevant examinations since October 2016. Each such examination was conducted at the LEAs' offices and only those parts of the interception products to which LEA officers had accessed previously would be examined by the Commissioner and his delegated officers.

2.25 Apart from some specific cases such as LPP and JM cases reported by the LEAs, the Commissioner would also select from the weekly reports, on the basis of the information provided therein or at random, interception products of other cases for examination with a view to checking if those other interception products may contain any LPP information, JM or any information that indicates heightened LPP/JM likelihood not reported by the LEAs. Such examination would also enable the Commissioner to identify whether there were any irregularities or

concealment of unauthorized acts violating the ICSO, such as checking if the person using the telecommunications facilities as authorized by a prescribed authorization was actually the subject of the prescribed authorization and if any discontinuance of interception operation was to avoid exposure or detection of inadvertent mistakes or acts done without authority. If there were questions or doubts arising from the examination of the interception products, the Commissioner would require the LEA concerned to provide clarification or explanation.

2.26 During the report period, with the basis of selection as mentioned in paragraph 2.25 above, the interception products of 427 selected authorizations had been examined. Of these 427 authorizations, no irregularity was found for 426 authorizations. As for the remaining authorization, it involved discrepancies made in submitting an REP-11 report to the panel judge as detailed in Case 6.7 of Chapter 6.

Counter-checking with non-LEA parties and through other means

2.27 Apart from checking the weekly returns from the LEAs against those from the PJO, and examining case files, documents and interception products at the LEAs' offices, other measures have also been adopted for further checking the interceptions conducted by the LEAs.

2.28 Wherever necessary, counter-checks were conducted with non-LEA parties such as CSPs who have played a part in the interception process but are independent from the LEAs. The interception of telecommunications facilities by an LEA is made through a dedicated team ('the Team') that, whilst being part of the LEAs, operates independently of their investigative arms. While the CSPs are required to furnish the Commissioner with a four-weekly return to ensure that the facilities intercepted tally with those as reported by the respective LEAs and to notify the Commissioner at once upon discovery of any unauthorized

interception, the Team has also archived in a confidential electronic record the status of all interceptions whenever they are effected, cancelled or discontinued. Arrangements have also been made for the archiving of the status of all interceptions being conducted at particular intervals as designated by the Commissioner from time to time. All these records are available to the Secretariat but only the Commissioner and his designated staff can access the confidentially archived information for the purpose of checking the intercepted facilities for their status of interception at various points of time and as at any reference point of time so designated by the Commissioner, ensuring that no unauthorized interception has taken place.

Results of various forms of checking

2.29 During the report period, there was no case of wrong or unauthorized interception revealed by the various forms of checking.

CHAPTER 3

COVERT SURVEILLANCE

Covert surveillance

3.1 Pursuant to section 2 of the ICSO, covert surveillance means any surveillance carried out with the use of any surveillance device if the surveillance is carried out in circumstances where the subject of the surveillance is entitled to a reasonable expectation of privacy, that it is carried out in a manner calculated to ensure that the subject is unaware that the surveillance is or may be taking place, and that it is likely to result in the obtaining of any private information about the subject. Surveillance device means a data surveillance device, a listening device, an optical surveillance device or a tracking device or a device that is a combination of any two or more of such devices. Any surveillance which does not satisfy the above criteria is not covert surveillance under the Ordinance.

Two types of covert surveillance

3.2 There are two types of covert surveillance: Type 1 and Type 2. Type 1 surveillance has a higher degree of intrusiveness into the privacy of the subject and requires a panel judge's authorization whereas an authorization for Type 2 surveillance, termed an executive authorization, can be issued by an authorizing officer of the LEA to which the applicant belongs. An authorizing officer is an officer not below the rank equivalent to that of Senior Superintendent of Police designated by the head of department.

Written applications

- 3.3 During the report period, there were a total of:
- (a) 22 written applications for Type 1 surveillance including 17 fresh and five renewal applications; and
 - (b) three written applications for Type 2 surveillance, all of which being fresh applications.
- 3.4 No application for Type 1 or Type 2 surveillance was refused.

Emergency authorizations

3.5 An officer of an LEA may apply in writing to the head of the department for the issue of an emergency authorization for any Type 1 surveillance, if he considers that there is immediate need for the Type 1 surveillance to be carried out due to an imminent risk of death or serious bodily harm of any person, substantial damage to property, serious threat to public security or loss of vital evidence, and having regard to all the circumstances of the case that it is not reasonably practicable to apply for the issue of a judge's authorization. An emergency authorization shall not last longer than 48 hours and may not be renewed. Where any Type 1 surveillance is carried out pursuant to an emergency authorization, the head of the department shall cause an officer of the department to apply to a panel judge for confirmation of the emergency authorization as soon as reasonably practicable after, and in any event within the period of 48 hours beginning with, the time when the emergency authorization is issued. During the report period, no application for emergency authorization for Type 1 surveillance was made by the LEAs.

3.6 On the other hand, there is no provision in the Ordinance for application for emergency authorization for Type 2 surveillance.

Oral applications

3.7 Applications for Type 1 and Type 2 surveillance, including those for emergency authorization, should be made in writing. Nonetheless, an application for the issue or renewal of a prescribed authorization may be made orally if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make a written application. The relevant authority may orally deliver his determination to issue the prescribed authorization or refuse the application.

3.8 The COP stipulates that the oral application procedure should only be resorted to in exceptional circumstances and in time-critical cases where the normal written application procedure cannot be followed. For a prescribed authorization orally granted for Type 1 surveillance, the head of the department shall cause an officer of the department to apply in writing to the panel judge, and for such an authorization for Type 2 surveillance, the applicant shall apply in writing to the authorizing officer, for confirmation of the orally granted prescribed authorization as soon as reasonably practicable and in any event within 48 hours from the issue of the authorization. Failing to do so will cause that orally granted prescribed authorization to be regarded as revoked upon the expiration of the 48 hours.

3.9 During the report period, no oral application for Type 1 or Type 2 surveillance was made by the LEAs.

Duration of authorizations

3.10 The maximum duration of prescribed authorizations (fresh authorizations as well as renewals) for Type 1 surveillance granted by the panel judge and Type 2 surveillance by the authorizing officers allowed under the Ordinance is three months. In the report period, the longest

approved duration of Type 1 surveillance granted was 31 days whereas the shortest one was about three days. Overall, the average duration for such authorizations was about 16 days. The duration of all the Type 2 surveillance granted was about seven days each.

Offences

3.11 The major categories of offences for the investigation of which prescribed authorizations were issued or renewed for surveillance during the report period are set out in Table 2(b) in Chapter 8.

Revocation of authorizations

3.12 During the report period, 18 Type 1 surveillance operations were discontinued under section 57 of the ICSO before the natural expiration of the prescribed authorizations. The grounds for discontinuance were mainly that the subject had been arrested or the surveillance had been carried out. Section 57(3) requires the LEA to report the discontinuance and the ground for discontinuance to the relevant authority who shall revoke the prescribed authorization concerned upon receipt of the report on discontinuance. Of these reported discontinuance cases, 14 prescribed authorizations were subsequently revoked fully by the panel judge under section 57. The remaining prescribed authorizations had already expired by the time the panel judge received the discontinuance reports. Thus, the panel judge could only note the discontinuance reported instead of revoking the prescribed authorizations.

3.13 As regards Type 2 surveillance, during the report period, three Type 2 surveillance operations were discontinued under section 57 before their natural expiration. The grounds for discontinuance of the operations were that the subject had been arrested, the anticipated meetings did not materialise or the LEA concerned needed to modify the

scope of the surveillance authorized. All the three prescribed authorizations concerned were subsequently revoked by the authorizing officer.

3.14 Revocation of authorizations is expressly provided for in section 58 of the ICSO for covert surveillance when the subject(s) of the covert surveillance has been arrested. During the report period, there were five Type 1 and one Type 2 surveillance operations involving LEAs being aware of the arrest of the subjects. The LEAs concerned were aware that 39 subjects of the Type 1 surveillance operations and one subject of the Type 2 surveillance operation had been arrested. The LEAs concerned did not seek continuation of prescribed authorizations by way of section 58 report to the relevant authority and the covert surveillance operations concerned were discontinued pursuant to section 57.

3.15 The LEAs' voluntary selection of the section 57 procedure to discontinue the covert surveillance operation as soon as reasonably practicable instead of resorting to the section 58 process of reporting an arrest with a wish to continue with the operation, similar to the situation for interception, demonstrates that the LEAs were appreciative of the risk of obtaining LPP information after an arrest.

Authorizations with five or more previous renewals

3.16 During the report period, no authorization for Type 1 or Type 2 surveillance had been renewed for more than five times.

Application for device retrieval warrant

3.17 During the report period, there was no application for any device retrieval warrant for retrieving the devices used for Type 1 or Type 2 surveillance, the reported reason being that the devices were

removed at the time of the completion of the surveillance operation, successful or otherwise.

Arrests attributable to covert surveillance

3.18 As a result of or further to surveillance operations, a total of 49 persons who were subjects of the prescribed authorizations were arrested. Sixteen non-subjects were also arrested in consequence of such operations.

Procedure of oversight for covert surveillance

3.19 The LEAs' compliance with the requirements of the Ordinance in respect of covert surveillance cases reported in 2019 was reviewed by the following ways:

- (a) checking of the weekly reports submitted by the LEAs and the PJO;
- (b) examination of the contents of the LEAs' files and documents during periodical visits to the LEAs;
- (c) examination of surveillance products at the LEAs' offices; and
- (d) checking of the records kept by the surveillance device recording system of the LEAs.

Details of the above reviews are set out in the ensuing paragraphs.

Checking of weekly reports

3.20 Weekly reports submitted by the LEAs and the PJO cover all statutory activities, including both types of covert surveillance. The way

of checking that has been described in Chapter 2 for interception equally applies to covert surveillance.

Examination of documents and information during periodical visits

3.21 The mechanism of checking cases during periodical visits to the LEAs is described in Chapter 2.

3.22 During the year, 30 applications for Type 1 surveillance (including 13 applications reported in 2018 and 17 in 2019) and 63 related documents/matters had been checked.

3.23 Pursuant to the Ordinance, an application for Type 2 surveillance is submitted to and determined by a designated authorizing officer of the department concerned. Special attention has all along been paid to examine each and every application for Type 2 surveillance to ensure that all such applications correctly fall within the category of Type 2 surveillance and all executive authorizations are granted properly. During the periodical visits to the LEAs in the report period, apart from the clarification of matters relating to minor discrepancies in the weekly reports, two applications for Type 2 surveillance and two related documents/matters had been checked.

3.24 For cases where surveillance devices have been withdrawn under a prescribed authorization but no surveillance operation is carried out, the Commissioner would examine the following matters:

- (a) whether the prescribed authorization should have been sought in the first place;
- (b) the reason for not carrying out any surveillance operation pursuant to the prescribed authorization;

- (c) whether the devices drawn were used during the period concerned for any purposes other than those specified in the prescribed authorization; and
- (d) the way in which the devices drawn were kept by officers before they were returned to the device store/registry.

Such cases are included for examination in the periodical visits, at which the relevant case documents are checked and the LEAs concerned are requested to answer queries where necessary. In the report period, the examination of these cases did not reveal any sign of surveillance devices being used for any unauthorized purposes.

3.25 During my checking of the relevant weekly report and the device register, I had certain queries on a covert surveillance case and required the LEA concerned to provide explanations during a periodical visit. Details of this case are set out in Case 6.13 of Chapter 6. As regards the other covert surveillance cases checked, they were found to be in order.

Examination of surveillance products

3.26 In accordance with section 53(1)(a) of the Ordinance, the Commissioner and his delegated officers have the express power to check the protected products obtained by the LEAs through covert surveillance. The examination of surveillance products was conducted at the LEAs' offices.

3.27 Apart from some specific cases such as LPP and JM cases, the Commissioner would also select from the weekly reports, on the basis of the information provided therein or at random, other cases for examination with a view to checking if the surveillance products of these cases may contain any LPP information, JM or any information that indicates heightened LPP/JM likelihood not reported by the LEAs. Such

examination would also enable the Commissioner to identify whether there were any irregularities or concealment of unauthorized acts violating the ICSO, such as checking if the person under covert surveillance as authorized by a prescribed authorization was actually the subject of the prescribed authorization, if any information subject to LPP in the surveillance products had been screened out by the dedicated units before the products were passed to the investigators, and if any discontinuance of surveillance operation was to avoid exposure or detection of inadvertent mistakes or acts done without authority. If there were questions or doubts arising from the examination of the surveillance products, the Commissioner would require the LEA concerned to provide clarification or explanation.

3.28 During the report period, the surveillance products of six selected authorizations were examined. Notwithstanding that one of these six authorizations involved an incident as detailed in Case 6.8 of Chapter 6 where there was an inaccuracy in the recorded time of a surveillance product, nothing untoward was found during the examination. Besides, other three authorizations had been selected for examination of their protected products but no checking was made as no surveillance operation had been conducted or no recording had been made during the surveillance operation.

Checking of surveillance devices

3.29 Having regard to the fact that covert surveillance, as defined by the Ordinance, is surveillance carried out with the use of one or more surveillance devices, the LEAs had been required to develop a comprehensive recording system of surveillance devices, so as to keep a close watch and control over the devices with a view to restricting their use only for authorized and lawful purposes. Not only is it necessary to keep track of surveillance devices used for ICSO purposes, but it is also necessary to keep track of devices capable of being used for covert

surveillance ('capable devices') albeit they may allegedly only be used for non-ICSO purposes. Capable devices should be kept under close scrutiny and control because of the possibility that they might be used without authorization or unlawfully. The LEAs have to maintain a register of devices withdrawn based on loan requests supported by a prescribed authorization and a separate register of devices withdrawn for administrative or other purposes based on loan requests for surveillance devices in respect of which no prescribed authorization is required. Both types of register will also record the return of the devices so withdrawn. An inventory list of surveillance devices for each device registry is also maintained with a unique serial number assigned to each single surveillance device item for identification as well as for checking purposes.

3.30 The LEAs have established a control mechanism for issuing and collecting surveillance devices. All records of issue and return of surveillance devices should be properly documented in the device register. Copies of both the updated inventory lists and device registers are submitted to the Commissioner regularly. Where necessary, the LEAs are also required to provide copies of the device request forms for examination. In case of discrepancies or doubts identified as a result of checking the contents of these copies and comparing them with the information provided in the weekly report forms and other relevant documents, the LEA concerned will be asked to provide clarification and explanation.

Visits to device stores

3.31 Apart from the checking of inventory lists and device registers of surveillance devices managed by the LEAs, the Commissioner would also make visits to the device stores of the LEAs for the following purposes:

- (a) to check the entries in the original registers against the entries in the copy of registers submitted to the Commissioner, with the aim to ensure that their contents are identical;

- (b) to check the procedures for the issue and return of surveillance devices for purposes under the Ordinance and for non ICSO-related usage;
- (c) to check whether any issue of device was appropriately supported by a request form;
- (d) to check the physical existence of items on the copy inventory entries provided to the Commissioner periodically;
- (e) to check the items of device shown in the copy registers to have been recently returned to ensure that they are being kept in the stores;
- (f) to make stock-check of items evidenced by the copy registers to be in the stores;
- (g) for the above purposes, to compare the unique number on each item as shown on the copy registers against the number assigned to the item as marked on it or attached to it; and
- (h) to view the items physically and be briefed, if need be, as to how they may be used for conducting covert surveillance operations.

3.32 During the report period, a total of four visits were made to the device stores of LEAs.

Removable storage media

3.33 To better control the issue and return of surveillance devices, all the LEAs have adopted computerised device management system ('DMS') in their device stores. In addition, the LEAs have adopted the use of tamper-proof labels to seal the removable storage media ('RSM') (e.g. memory cards, discs and tapes) inside the surveillance devices at the time

of issue to avoid any possibility of these RSM being substituted, or in any way tampered with. The LEAs have also adopted the use of QR Code to facilitate the issue and return of the RSM through DMS. Information showing whether RSM is issued or returned with a surveillance device and whether the tamper-proof label sealing the RSM inside the device is intact upon return of the device were clearly documented in the device register.

Devices for non-ICSO purposes

3.34 As a matter of practice, an authorized covert surveillance should always be supported by a prescribed authorization issued by a relevant authority but a non-ICSO operation requiring issue of devices will not have that support. Hence, in keeping track of issue of surveillance devices for non-ICSO purposes, the LEAs have accepted the requirements that a two-level approval by way of an endorsement of an officer and an approval of a senior officer is required. Both officers will sign with date on a device request memo to signify their endorsement and approval respectively. Each device request memo should have a unique memo reference. The withdrawing officer will bring along the device request memo to the device registry where the storekeeper on duty will issue the surveillance devices requested.

3.35 During the year, one report relating to surveillance devices for non-ICSO purposes was received from an LEA. Details of this case are described below.

Mistakes in making movement records of a surveillance device issued for a non-ICSO operation in the DMS

3.36 An LEA reported to me an incident in which some mistakes were made in the DMS in respect of the movement records of a surveillance device issued for a non-ICSO operation.

3.37 Some surveillance devices issued initially for a non-ICSO operation were redeployed for use in either one of the other two non-ICSO operations ('Operation A' and 'Operation B'). While one surveillance device ('Device X') was redeployed to Operation A, the others were redeployed for use in Operation B. When the device storekeeper concerned ('the Device Storekeeper') recorded the redeployment of the surveillance devices in the DMS, he made a wrong remark in the record of Device X that it was redeployed to Operation B. The mistake was later rectified by another device storekeeper during his random check on the documentary record.

3.38 All the surveillance devices were returned to the device store on the same day when they were issued. In processing return of Device X, the Device Storekeeper forgot to scan the barcode of the surveillance device before putting it in a cabinet for storage, resulting in omission of a return record of Device X in the DMS. A week later, the supervisor of the Device Storekeeper, when checking the relevant device register, found the absence of the return record of Device X. The supervisor interviewed all the relevant officers immediately. Having confirmed the return of Device X on that day, the supervisor made a retrospective record in the DMS for the return of the surveillance device. However, the supervisor used a wrong function of the DMS to record the return. According to the relevant guidelines, the function used by the supervisor in making retrospective records of the movement of surveillance devices should only be used in certain situations, which did not include the one in question.

3.39 The LEA concluded that the mistakes were caused by carelessness of the Device Storekeeper or his supervisor without any foul play or ulterior motive. The LEA proposed to issue a verbal advice (non-disciplinary) to both officers to remind them of the need to be more vigilant in operating the DMS in future. The LEA was also making an enhancement to the DMS to better keep track of the return of surveillance devices. Having reviewed the case, I agreed that no foul play or ulterior

motive was involved in the incident since there was no good reason for the two officers to make the mistakes intentionally. The proposed actions against the two officers and the enhancement to the DMS were considered appropriate.

CHAPTER 4

LEGAL PROFESSIONAL PRIVILEGE AND JOURNALISTIC MATERIAL

Obligations of LEAs regarding LPP cases

4.1 The Ordinance requires that when making an application for a prescribed authorization, the applicant should state in the affidavit or statement in writing the likelihood that any information which may be subject to LPP will be obtained by carrying out the interception or covert surveillance.

4.2 The COP provides that the LEA should notify the Commissioner 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 LEA's notification, the Commissioner may review the information passed on to the investigators to check that it does not contain any information subject to LPP that should have been screened out.

4.3 For each of these cases, there are procedures to be followed at different stages of the operation. When making an application for a prescribed authorization, the LEA applicant is obligated to state his assessment of the likelihood of obtaining LPP information. If subsequently there is anything that transpires which may affect the assessment, which is considered as a material change in circumstances, the officer concerned has to promptly report to the relevant authority the altered LPP assessment. The reporting requirement regarding material change in circumstances is stipulated under section 58A of the ICSO. The report to the panel judge is made by way of an REP-11 report; or, in the case of a Type 2 surveillance operation, by way of an REP-13 report to the

authorizing officer. If the subject of the interception or covert surveillance has been arrested and the officer concerned considers that the operation should continue, the officer should submit a section 58 report to the relevant authority assessing the effect of the arrest on the likelihood that any LPP information will be obtained by continuing the interception or covert surveillance. In the report made under section 58A or section 58, the officer has to provide the details of all relevant circumstances, including why the assessment has altered, how it has come about to consider that LPP information has been obtained or may likely be obtained, the details of the likely LPP information that has been obtained, and what steps have been taken or are proposed to take to prevent infringement of the right to communications that are protected by LPP. In order to apprise the Commissioner promptly with timely information on this important matter, the concerned LEA is required to give the Commissioner a similar notification of each of such occurrences in accordance with the COP.

4.4 Regarding cases with assessment that there was likelihood of involving LPP information, the panel judge would impose additional conditions if he granted the authorization or allowed it to continue. These additional conditions were stringent and effective in safeguarding the important right of individuals to confidential legal advice.

4.5 There is a set of reporting and preservation requirements for cases involving LPP information. In particular, for interception operations involving telephone calls, when an LEA encounters a call with heightened LPP likelihood or LPP information, the LEA is required to submit an REP-11 report to the panel judge in respect of this call. This is named 'Reported LPP Call' irrespective of whether LPP information has indeed been obtained. The reporting officer has to disclose in the report the number of times the Reported LPP Call has been listened or re-listened to, the respective date and time and duration of each such listening or re-listening and the identity of each of the listeners. In addition, in the

report to the Commissioner, the reporting officer should also state whether there are any other calls between the telephone number involved in the Reported LPP Call and the subject's telephone number under interception, irrespective of whether such calls are intercepted before or after the Reported LPP Call. If there are such 'other calls', the reporting officer is also required to provide information on whether they have been listened to and if so, for how long and the identity of the listeners. In order to provide such information, the reporting officer should consult the relevant audit trail report ('ATR') that records accesses to the intercepted calls together with the corresponding call data when preparing the REP-11 report and the notification to the Commissioner. For LPP cases involving interception, the LEA should preserve all the interception products which are still available at the time of discovery of LPP likelihood, heightened LPP likelihood or LPP information, the transcripts, summaries, notes, ATRs, etc. The preserved records should not be destroyed without the prior consent of the Commissioner as stated under section 59(1)(c) of the Ordinance. LEAs are required to make similar reporting and preservation arrangements also for cases where JM is involved or likely to be involved.

4.6 In the event that LPP information has been inadvertently obtained in covert surveillance operations, the COP also provides that investigators monitoring the operations will be required to hand over the recording to a dedicated unit who will screen out any information subject to LPP before passing it to the investigators for their retention. The Commissioner should be notified. On the basis of the LEA's notification, the Commissioner may review the information passed on by the dedicated unit to the investigators to check that it does not contain any information subject to LPP that should have been screened out. Similarly, the dedicated unit is required to screen out any JM that has been inadvertently obtained and withhold such materials from the investigators.

Outstanding LPP cases in 2018

4.7 As reported in paragraphs 4.10 and 4.15 of the Annual Report 2018, there was an LPP case which was discontinued in 2018 and related to non-compliance detected by me in early 2019. Details of this case are set out in Case 6.1 of Chapter 6.

4.8 Besides, it was reported in paragraph 4.16 of the Annual Report 2018 that there were 29 cases of heightened LPP likelihood which were still on-going beyond 2018. The authorized operations of these 29 cases were discontinued in 2019 and I had completed the review of these cases in the report period. Other than one case which involved an incident of technical problem of the computer systems mentioned in paragraph 6.130 of the Annual Report 2018 and another case which was related to the incident referred to in Case 6.3 of Chapter 6, nothing untoward was revealed by various forms of checking of these LPP cases.

LPP reports received in 2019

4.9 In the report period, LEAs submitted notifications, in accordance with the COP, on 170 new cases that were likely to involve LPP information (LPP cases).

4.10 Amongst these 170 new LPP cases, 18 cases were assessed at the time of application that the operations sought to be authorized would likely obtain information subject to LPP and the panel judge imposed additional conditions in the prescribed authorizations in all these cases. There was no subsequent change in circumstances one way or another relating to LPP likelihood for these 18 cases.

4.11 For the remaining 152 cases ^{Note 1}, the LEAs submitted REP-11 or section 58 reports to the panel judge on the subsequent change in circumstances relating to LPP involvement or likelihood. These 152 cases included:

- (a) one case of obtaining information suspected to be subject to LPP; and
- (b) 151 cases of heightened likelihood of obtaining LPP information:
 - (i) in 112 cases the panel judge allowed the continuation of the prescribed authorization subject to additional conditions imposed to guard against the risk of obtaining LPP information; and
 - (ii) in 39 cases the concerned LEA discontinued the operations of its own accord.

4.12 Of the 170 new LPP cases, the authorized operations for 155 cases were discontinued in the report period. I had completed the review of these 155 cases. In the review of these LPP cases, all the relevant documents and records including the prescribed authorization, the REP-11 report, section 58 report, the determination by the panel judge, the notes, the summaries, the communication data, the ATRs, etc. were checked by me and my staff. For cases where the panel judge allowed the prescribed authorizations to continue subject to additional conditions, we checked whether the LEAs had complied with the additional conditions imposed by the panel judge, whether the LPP information or likely LPP information had been screened out from the summaries passed on to investigators. In respect of interception of telephone calls, we also checked whether there were calls between the same telephone numbers

^{Note 1} Some of these cases were assessed at the time of application that the operations sought to be authorized would likely obtain information subject to LPP and some were not.

preceding the Reported LPP Call that should have been but had not been reported, and whether there was any listening or re-listening to the interception products after the discontinuance or revocation of the prescribed authorizations.

4.13 The protected products of the 155 LPP cases were also examined by me and my delegated officers. When examining these products (and also those for JM cases), we particularly checked the following:

- (a) whether the contents of the communications or information reported in the relevant REP-11 report and notification to the Commissioner tallied with what was listened to or viewed by the LEA officers; and
- (b) whether there was any other communication or information that was subject to LPP or indicated heightened LPP likelihood (or contained JM or indicated heightened JM likelihood) but had not been reported to the relevant authority.

One case of obtaining information suspected to be subject to LPP

4.14 The case where the LEA concerned reported the obtainment of information suspected to be subject to LPP involved a Type 1 surveillance. At the grant of the prescribed authorization concerned, the surveillance operation was assessed to have a likelihood of obtaining LPP information. The panel judge imposed additional conditions on the prescribed authorization to guard against the risk of obtaining LPP information.

4.15 The LEA carried out covert surveillance operations on two days. On the second day, surveillance was conducted on a meeting. Shortly after the meeting, the crime investigation was turned overt and the LEA discontinued the Type 1 surveillance.

4.16 Later the same day, the surveillance products obtained from the meeting were handed over to the dedicated unit for screening. From the screening on one of the surveillance products, an officer of the dedicated unit found that at the last few minutes of the meeting, the subject said something which contained information that was suspected to be subject to LPP. The LEA submitted to the panel judge an REP-11 report and a discontinuance report, with the contents of the suspected LPP information detailed separately in an annex to the REP-11 report. The annex was placed in a separate sealed envelope for opening by the panel judge personally. The panel judge noted the REP-11 report and duly revoked the prescribed authorization. A similar notification with a copy of the REP-11 report and the discontinuance report was submitted to me.

4.17 I reviewed the case and did not find any irregularities. As regards the information suspected to be subject to LPP, I had examined the recording and considered that LPP information had been inadvertently obtained. The record stated in the annex of the REP-11 report was correct. I also checked and confirmed that the information passed on to the investigators did not contain any information subject to LPP that should have been screened out.

139 cases of heightened LPP likelihood and 15 cases of assessed LPP likelihood

4.18 The review of the 154 heightened/assessed LPP likelihood cases had been conducted in accordance with the mechanism as stated in paragraphs 4.12 and 4.13 above. Of these 154 cases, eight cases were related to the incidents referred to in Cases 6.4, 6.5 ^{Note 2}, 6.6, 6.9, 6.10, 6.11 and 6.12 and one case involved an incident of technical problem of the computer systems mentioned in paragraph 6.82 of Chapter 6. Nothing untoward was found for the remaining 145 cases.

Note 2 This incident involved two LPP cases.

15 on-going cases of heightened/assessed LPP likelihood

4.19 As the authorized operations for 15 cases of heightened/assessed LPP likelihood reported in 2019 are still on-going beyond the report period, details about my review of these cases will be reported in the next annual report.

Obligations of LEAs regarding JM cases

4.20 The Ordinance requires the LEA applicant to set out, at the time of applying for a prescribed authorization, the likelihood that any information which may be the contents of any JM will be obtained by carrying out the interception or covert surveillance sought to be authorized. The COP provides that the LEAs should notify the Commissioner of cases where information which may be the contents of any JM has been obtained or will likely be obtained through interception or covert surveillance operations. The reporting, preservation and screening requirements for cases involving JM are as those set out in paragraphs 4.5 and 4.6 above.

JM reports received in 2019

4.21 In 2019, I received notifications on five new cases with heightened likelihood of obtaining JM submitted in accordance with the COP, for which REP-11 reports were submitted to the panel judge.

Five cases of heightened JM likelihood

4.22 The five cases of heightened likelihood of obtaining JM included:

- (a) four cases which the panel judge imposed additional conditions on the prescribed authorizations after receipt of the REP-11 reports; and
- (b) one case which the LEA concerned discontinued the operation of its own accord.

4.23 I conducted a review of all the five JM cases in accordance with a mechanism which was similar to that of checking LPP cases as detailed at paragraphs 4.12 and 4.13 above.

4.24 Checking of the relevant documents and records of these five heightened JM likelihood cases did not reveal any irregularity. The protected products were also checked and nothing untoward was found. In these five cases and during the report period, no JM was actually obtained.

Examination of the protected products in past cases

4.25 Apart from cases reported in the report period, since October 2016, the Commissioner and his delegated officers have also examined the protected products of LPP/JM cases that were reported before 2016. In the report period, preserved protected products of six LPP cases that were reported before 2016 had been checked. Nothing untoward was found for these six cases.

CHAPTER 5

APPLICATION FOR EXAMINATION AND NOTIFICATION TO RELEVANT PERSON

Application for examination

5.1 Pursuant to section 43 of the Ordinance, a person may apply in writing to the Commissioner for an examination if he suspects that he is the subject of any interception or covert surveillance activity carried out by officers of the LEAs. Upon receiving an application, the Commissioner shall carry out an examination to determine:

- (a) whether or not the suspected interception or covert surveillance has taken place; and
- (b) if so, whether or not such interception or covert surveillance has been carried out by an officer of an LEA without the authority of a prescribed authorization,

unless the Commissioner refuses to carry out an examination by reason of section 45(1) of the Ordinance. After the examination, if the Commissioner finds the case in the applicant's favour, he shall notify the applicant and initiate the procedure for awarding payment of compensation to him by the Government.

5.2 The circumstances provided in section 45(1) that justify the Commissioner not carrying out an examination are that, in the opinion of the Commissioner, the application is received by him more than one year after the last occasion on which the suspected interception or covert surveillance is alleged to have taken place, that the application is made anonymously, that the applicant cannot be identified or traced after the use of reasonable efforts, and that the application is frivolous or vexatious or

is not made in good faith. Section 45(2) of the Ordinance mandates the Commissioner not to carry out an examination or proceed with the examination where, before or in the course of the examination, he is satisfied that any relevant criminal proceedings are pending or are likely to be instituted, until the criminal proceedings have been finally determined or finally disposed of or until they are no longer likely to be instituted. Section 45(3) of the Ordinance defines relevant criminal proceedings as those where the interception or covert surveillance alleged in the application for examination is or may be relevant to the determination of any question concerning any evidence which has been or may be adduced in those proceedings.

The procedure

5.3 The procedure involved in an examination can be briefly described below. Enquiries will be made with the particular LEA which, the applicant alleges, has carried out either interception or covert surveillance or a combination of both against him as to whether any such statutory activity has taken place, and if so the reason why. Enquiries will also be made with the PJO as to whether any authorization had been granted by any panel judge for the particular LEA to carry out any such activity, and if so the grounds for so doing. Enquiries with other parties will be pursued if that may help obtain evidence regarding the existence or otherwise of any such alleged statutory activity. The results obtained from the various channels will be compared and counter-checked to ensure correctness. Apart from the information given above, it is considered undesirable to disclose more details about the methods used for the examination of applications or about the examinations undertaken, because that would possibly divulge information that may prejudice the prevention or detection of crime or the protection of public security.

5.4 The applications for examination will have to satisfy the following requirements, namely:

- (a) there is suspicion of interception of communications or covert surveillance that has been carried out against the applicant; and
- (b) the suspected interception or covert surveillance is suspected to have been carried out by one or more of the officers of the LEAs under the Ordinance, namely, Customs and Excise Department, Hong Kong Police Force, Immigration Department and Independent Commission Against Corruption.

5.5 A number of applicants did not understand the basis of an application for examination under the Ordinance. Some applicants alleged that they had been surreptitiously or openly followed or stalked by officers of an LEA. This normally would not satisfy the proper basis for an application for examination because there was no suspicion of any surveillance device being used. There have been cases previously where the applicants said devices suspected to be used included those which could directly read or control their minds. These again did not form a proper basis for an application to initiate an examination, the reason being that the devices suspected to be used do not fall within the kind or type of devices under the Ordinance the use of which would constitute a covert surveillance.

5.6 Some applicants described how a particular person, as opposed to an LEA officer, carried out the suspected interception or covert surveillance. This would also fail to satisfy the second requirement to entertain an application or to engage in an examination.

5.7 The above information concerning the relevant provisions of the Ordinance, application requirements and procedure as well as the consent form on the use of personal data have been provided on the website of the Secretariat. In addition, guidelines containing the

necessary information for making an application are available in the Secretariat office for prospective applicants.

Applications received in 2019

5.8 During the report period, there were 17 applications for examination. Of these applications, one application was received by me more than one year after the day on which the interception or covert surveillance was alleged to have taken place which came within the ambit of the exception covered by section 45(1) and could not be entertained. Six applications were subsequently not pursued by the applicants. Of the remaining ten applications, four alleged interception and six claimed a combination of interception and covert surveillance. Since none of these ten applications came within the ambit of the exceptions covered by section 45(1) or section 45(2), I carried out an examination provided for in section 44 of the Ordinance in respect of each case.

5.9 After making all necessary enquiries, I found all the ten cases not in the applicants' favour and accordingly notified each of the applicants in writing of the findings, with five of such notices issued during the report period and five thereafter. By virtue of section 46(4) of the Ordinance, the Commissioner is not allowed to provide reasons for his determination or to inform the applicants whether or not the alleged or suspected interception or covert surveillance had indeed taken place.

Notification to relevant person

5.10 Section 48 of the Ordinance obliges the Commissioner to give notice to the relevant person whenever, during the performance of the functions under the Ordinance, the Commissioner discovers any interception or covert surveillance carried out by an officer of any one of the four LEAs covered by the Ordinance without a prescribed authorization. However, section 48(3) provides that the Commissioner

shall only give a notice when he considers that doing so would not be prejudicial to the prevention or detection of crime or the protection of public security. Section 48(6) also exempts the Commissioner from his obligation if the relevant person cannot, after the use of reasonable efforts, be identified or traced, or where he considers that the intrusiveness of the interception or covert surveillance on the relevant person is negligible.

5.11 Consideration of the application of section 48 may arise under a number of situations. For example, the interception of telephone communications on a telephone number other than that permitted by a prescribed authorization issued by a panel judge constitutes an unauthorized interception. The Commissioner will then consider whether he should, as obliged by section 48 of the Ordinance, give a notice to the relevant person of the wrong interception. If and when the notice is given, the relevant person will be invited to make written submissions in relation to the assessment of reasonable compensation to be paid to him by the Government.

5.12 During the report period, no notice pursuant to section 48 of the Ordinance was issued.

Prohibition against disclosure of reasons for determination

5.13 Section 46(4) expressly provides that in relation to an application for examination, the Commissioner is not allowed to provide reasons for his determination, or give details of any interception or covert surveillance concerned, or in a case where he has not found in the applicant's favour, indicate whether or not the suspected interception or covert surveillance has taken place.

5.14 During the year, I have observed that there were occasions where the applicants expressed strong discontent at not being given the details of the reasons for my determinations. It is hoped that the public

will understand that this statutory prohibition is designed to forbid the disclosure of any information which might prejudice the prevention or detection of crime or the protection of public security, preventing any advantage from being obtained by criminals or possible criminals over the LEAs in the latter's efforts in fighting crimes and in protecting the safety of the community in Hong Kong. There should not be any doubt that the Commissioner carries out his duties and functions under the Ordinance with the utmost good faith and sincerity.

CHAPTER 6

NON-COMPLIANCE, IRREGULARITIES AND INCIDENTS

Reporting of non-compliance, irregularities and incidents

6.1 By virtue of section 54 of the Ordinance, where the head of any 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, he is obliged to submit to the Commissioner a report with details of the case (including any disciplinary action taken in respect of any officer). The head of any LEA is also required to submit to the Commissioner a report with details of the case even if the failure to comply with any relevant requirement is not due to the fault of the LEA or any of its officers. Relevant requirement is defined in the Ordinance to mean any applicable requirement under any provision of the ICSO, the COP, or any prescribed authorization or device retrieval warrant concerned.

6.2 Besides, there is a mechanism on reporting and monitoring of covert operations in place whereby the LEAs are required by the Commissioner to report cases of irregularity or even simply incidents which are not covered by section 54 of the Ordinance for his consideration and scrutiny so that any possible non-compliance will not escape his attention.

6.3 For cases of non-compliance, irregularity or incident discovered upon examination of documents, information and protected products during visits to LEAs, the LEA concerned is required to investigate the matter and submit a report or provide explanation to the Commissioner.

6.4 When reporting, normally the LEAs would adopt a two-step approach. They would first submit an initial report upon discovery of the event, to be followed by a full investigation report after an in-depth investigation into the case.

Outstanding cases brought forward from Annual Report 2018

6.5 In my Annual Report 2018, there were two outstanding cases. They are dealt with in the ensuing paragraphs.

Outstanding case (i): An incident report relating to section 61 of the ICSO [Paragraph 6.6 of Annual Report 2018]

6.6 This incident was first reported by an LEA in late 2014. The court proceedings that were relevant to the incident have not concluded at the time of writing this report. The reporting of this case can only be made when the relevant court proceedings have concluded to avoid the risk of prejudicing the administration of justice.

Outstanding case (ii) : Conducting surveillance operation not in compliance with the prescribed authorization [Paragraph 6.106 of Annual Report 2018]

6.7 The case concerned was a Type 1 surveillance which took place in 2018. It was selected for checking from the weekly report. Checking of the protected products of the case revealed that certain periods of the surveillance were/might be conducted outside the ambit of the prescribed authorization. This case was briefly reported in paragraph 6.106 of the Annual Report 2018.

6.8 A prescribed authorization was applied for by the LEA concerned to conduct Type 1 surveillance on a subject. In granting the

application, the panel judge required the subject to be present in the specified premises when the surveillance was carried out.

6.9 The Divisional Head in charge of the operation ('Officer A') of the LEA concerned wrongly interpreted the term and failed to make operational arrangement to ensure compliance with the term.

6.10 During the inspection visits to the LEA to examine the relevant documents and protected products obtained from the surveillance operation, I found that there were occasions where surveillance was conducted when the subject was not present in the specified premises, which was not in compliance with the term of the prescribed authorization. I requested the LEA to give a full account on the arrangement in conducting the surveillance operation.

6.11 The LEA stated in the investigation report that at certain periods of the surveillance operation conducted, the subject was not inside the specified premises, which was not in compliance with the term laid down by the panel judge in the prescribed authorization.

6.12 The LEA commented that Officer A was not aware of any potential non-compliance in the operation prior to the observation made by me during my inspection visit. There was no evidence of any willful or deliberate breach of the term set, or any attempt of concealment of such non-compliance. In the reviewing process of this surveillance operation, two senior officers ('Senior Officer B' and 'Senior Officer C') were involved and both of them were in acting capacities at the material time. The LEA pointed out in the investigation report that both of them were not familiar with the surveillance duties in their daily work. Due to the lack of relevant experience in surveillance operations, they failed to detect the non-compliance in the reviewing process.

6.13 The LEA proposed to give a verbal warning (disciplinary) to Officer A for her lack of vigilance and failure in seeking verification of her

understanding of the term pertaining to the Type 1 surveillance authorization, resulting in unauthorized surveillance being carried out in certain periods, a verbal advice (disciplinary) to Senior Officer B for his failure to detect the non-compliance in the reviewing process, given that the review file was routed through him to Senior Officer C, and a verbal advice (disciplinary) to Senior Officer C for his failure to detect the non-compliance in the reviewing process.

6.14 I have reviewed the case. The misinterpretation of the term of the concerned prescribed authorization by Officer A consequentially affected the execution arrangement of the surveillance operation. The lack of adequate and proper arrangement in ensuring that the subject was inside the specified premises when the surveillance operation took place led to possible situation of non-compliance.

6.15 There was one period of unauthorized surveillance supported by evidence. There were also several periods of suspected non-compliance which could not be further verified due to existence of constraints.

6.16 While I had no objection to the comment in the investigation report that there was no evidence to suggest any concealment of the unauthorized surveillance by any of the officers concerned, I considered the reviewing process of the surveillance operation conducted by Senior Officer B and Senior Officer C undesirable and disappointing. The mistakes made were left unnoticed after going through two levels of review. One major reason was that both reviewing officers were in acting capacities at the material time and were not familiar with the covert surveillance duties in their normal daily work. During the reviewing process, it was unsatisfactory that they only went through the doubtful areas with Officer A without seeking additional advices/views from the relevant team.

6.17 I considered the proposed disciplinary action against Officer A too lenient and requested the LEA to review it while the proposed disciplinary actions against Senior Officer B and Senior Officer C were considered proportionate. After review, the LEA proposed that on top of a verbal warning (disciplinary), Officer A would also be removed from ICSO related duties. Having considered the appropriateness and deterrent effect of the proposed action, I accepted the LEA's proposal.

6.18 As a remedial measure, the LEA had proposed enhanced training on the related surveillance topic to all officers in the relevant units and training on ICSO related duties be extended to officers who would have a role to play in the ICSO regime when acting up. Officers in acting capacities required to discharge ICSO functions had also been reminded to seek assistance in case of any doubt on ICSO matters. I considered the proposed measures appropriate and necessary.

Cases occurring in 2019

6.19 In 2019, there were 16 cases of non-compliance/irregularity/incident while none of them involved report submitted under section 54 of the Ordinance. The review of 15 cases had been completed and details of the review are set out below. For the remaining case, as the review is still on-going, details about my review will be reported in the next annual report.

Case 6.1 : Listening to a call involving a prohibited telephone number

6.20 The non-compliance in this case was discovered by me in early 2019 during review of a case of heightened likelihood of obtaining LPP information referred to in Chapter 4 of my Annual Report 2018.

6.21 At the grant of the prescribed authorization concerned, the interception operation was not assessed to have a likelihood of obtaining

LPP information. As the interception progressed, one day, an officer of the LEA concerned listened to part of a call and found that the call contained information which indicated heightened LPP likelihood. The panel judge, having considered the REP-11 report submitted by the LEA, allowed the prescribed authorization to continue with additional conditions imposed to guard against the risk of obtaining LPP information. One of the additional conditions was that officers of the LEA should refrain from accessing interception products involving a specified telephone number ('the prohibited number'). In order to comply with this additional condition, the LEA input the prohibited number into the relevant computer system, which would debar officers from accessing all the interception products involving the prohibited number.

6.22 In the course of my review of the LPP case, I found that, after the imposition of the additional conditions, one call involving the prohibited number was listened to by an officer for two seconds. It was a breach of the additional condition mentioned above. I requested the LEA to conduct an investigation into the matter and inform me of the outcome.

6.23 The investigation by the LEA found that the incident was due to a system bug, resulting in the failure of the computer system to screen out all the interception products involving the prohibited number under certain circumstances. As the computer system had always been very reliable, the officer concerned did not expect the malfunction of the computer system and listened to the call inadvertently. In this regard, the LEA considered that the officer should not be held responsible for the incident and proposed not to take any disciplinary action against the officer. To prevent recurrence of similar incidents, immediate actions were taken to resolve the computer problem.

6.24 In reviewing the case, I listened to the call in question, which confirmed that it did not contain any information subject to LPP or

information indicating heightened LPP likelihood. I noted the LEA's findings and considered the proposal of not taking any disciplinary action against the officer acceptable.

Case 6.2 : Incorrect user identity stated in the ATRs in respect of monitoring of interception by an officer

6.25 An LEA reported to me an incident where the user identity stated in the ATRs in respect of monitoring of interception by an officer was incorrect.

6.26 To carry out monitoring of interception, officers of the LEA are required to use their access cards to log in the relevant monitoring systems. One day, an officer ('Officer A') found that her access card malfunctioned. The card was, therefore, sent to another officer ('Officer B') for resetting. As one of the steps to reset an access card in the relevant computer system, the user identity should be selected from a list of users and then assigned to the access card. In resetting the access card of Officer A, Officer B wrongly selected the user identity which came immediately below that of Officer A in the list of users. However, Officer B was not aware of the mistake and then completed the remaining steps to reset the access card. After the access card was reset, Officer A used it to log in a system to conduct monitoring of interception. After successful login, the user identity popped up in the screen for about two seconds, but Officer A did not notice that it was not her identity. A few hours later, Officer A logged in again to conduct monitoring of interception and discovered the mistake. She reported the matter to her supervisor immediately. As a result of the mistake, the user identity shown in the ATRs in respect of the monitoring of interception by Officer A for the period concerned was wrong.

6.27 The investigation by the LEA concluded that no bad faith or ulterior motive was involved in the incident. The LEA proposed that both Officer A and Officer B be verbally advised (non-disciplinary) to be more vigilant in performing ICSO duties. To prevent recurrence of similar

incidents, an enhancement measure was implemented in the computer system concerned.

6.28 Having reviewed the case, I agreed that no bad faith or ulterior motive was involved in the incident since there was nothing to be gained by Officer B in wrongly selecting the user identity of Officer A when resetting the access card of Officer A. I considered the action taken against the two officers concerned as well as the enhancement measure in the computer system appropriate.

Case 6.3 : Delay in reporting an alias of the subject which surfaced during interception

6.29 The non-compliance was related to a case of heightened likelihood of obtaining LPP information mentioned in paragraph 4.8 of Chapter 4.

6.30 At the grant of the relevant prescribed authorization, the identity of the subject was already known by the LEA concerned. As the interception progressed, one day, an officer of the LEA listened to a call, which revealed an alias of the subject ('the first alias'). The officer reported such to his supervisor, who undertook to report this newly surfaced alias to the panel judge as a material change in the circumstances as required by section 58A of the Ordinance and paragraph 116 of the COP. However, the supervisor forgot to do so.

6.31 Several months later, another alias of the subject ('the second alias') was revealed in a message intercepted. Having been informed of such, the supervisor reviewed the relevant transcripts for preparation of an REP-11 report to be submitted to the panel judge to report on the second alias. During the review of the transcripts, the supervisor noted that the first alias was mentioned in a transcript in respect of a conversation. He then recalled that he had forgotten to submit an REP-11 report to the panel judge to report on the first alias discovered several

months ago. The supervisor reported the matter to his senior immediately. Subsequently, an REP-11 report was submitted to the panel judge to report on the two aliases of the subject. The LEA reported the matter to me through an initial report, followed by a full investigation report.

6.32 The investigation by the LEA concluded that the delay in reporting the first alias was due to a momentary lapse of mind of the supervisor and there was no foul play or ulterior motive involved. The LEA proposed to give a verbal advice (disciplinary) to the supervisor for his lack of vigilance in making a timely report to the panel judge on the change in the circumstances. To prevent recurrence of similar incidents, the LEA strengthened the procedures for the reporting of the identity or alias of the subject.

6.33 As required under section 58A of the Ordinance and paragraph 116 of the COP, the reporting of an alias of the subject should be made as soon as reasonably practicable. In this case, the panel judge was reported on the first alias several months after it surfaced. This was a non-compliance with the provision of the Ordinance and the COP. Having reviewed the case, I agreed that no foul play or ulterior motive was involved in the delay in reporting the first alias since the full identity of the subject was already known to the LEA at the outset and so nothing was to be gained by the delay in reporting the alias. The proposed disciplinary action against the supervisor and the revised procedures for the reporting of the identity or alias of the subject were considered appropriate.

Case 6.4 : Delay in reporting the previous arrest of the subject

6.34 An LEA reported to me an incident of delay in reporting to the panel judge on the previous arrest of the subject. This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.

6.35 Two prescribed authorizations were granted respectively for interception on two subjects, whose identities were not known by the LEA at the time of applying for the authorizations. As the interception progressed, one day, the LEA learnt of the identities of the two subjects and found that they were the same person. Having checked the relevant computer record, the investigation team of the LEA did not find any outstanding case in respect of any arrest of the subject and informed the interception unit of the checking result accordingly. Two days later, the interception unit submitted REP-11 reports to the panel judge to report the identity of the subject. Later on the same day, when reviewing the relevant investigation documents, a senior officer of the investigation team found that the subject was, indeed, being on bail in connection with his arrest which happened about one month before. The arrest was unrelated to the offence for which the interception operations were authorized to investigate. Subsequently, the LEA submitted to the panel judge section 58 reports to report the arrest status of the subject and REP-11 reports to report the non-reporting of the subject's arrest status in the REP-11 reports submitted before. The panel judge allowed the authorizations to continue with additional conditions imposed to guard against the risk of obtaining LPP information.

6.36 The investigation by the LEA found that the incident was mainly due to the carelessness of an officer, who mistook the status in respect of the subject's arrest when checking the relevant computer record. The officer checked the computer record cursorily and construed wrongly that the subject had been released and had no outstanding case. The officer reported the wrong checking result to her supervisor verbally. Based on the officer's verbal report, the supervisor, without counter-checking the relevant investigation record, submitted a written report via the senior officer (who discovered the mistake two days later) to the interception unit that the subject had no outstanding case. As a result, no section 58 report was submitted by the interception unit to

report the arrest status of the subject at the same time when the identity of the subject was reported to the panel judge.

6.37 The LEA concluded that no foul play or ulterior motive was involved in the incident. The LEA proposed to give a verbal warning (disciplinary) to the officer and the supervisor for their carelessness or oversight. The LEA also proposed to give a verbal advice (disciplinary) to the senior officer given his supervisory accountability.

6.38 I have reviewed the case. There was no evidence to contradict the findings of the LEA that there was no foul play or ulterior motive involved in the incident. The proposed disciplinary actions against the officers concerned were considered appropriate.

Case 6.5 : Interruption of interception of telecommunications facilities

6.39 The interception of telecommunications facilities by an LEA is made through a dedicated team ('the Team') that, whilst being part of the LEAs, operates independently of their investigative arms. The Team reported to me an incident in which the telecommunications interception of three facilities was inadvertently discontinued due to a human error. Two cases of heightened likelihood of obtaining LPP information referred to in Chapter 4 were involved in the incident.

6.40 The renewal of prescribed authorizations for the interception of the three facilities was granted by the panel judge on the day before the authorizations were to expire. The LEA concerned then passed the relevant documents to the Team. The Team was required to input details of the renewals to the relevant computer system on the same day or otherwise the interception would be discontinued automatically. However, upon receiving the relevant documents from the LEA, the duty officer of the Team failed to process the renewals on the computer system on that day as she was engaged in other urgent commitments. On the

next day, when the duty officer recalled that she had not performed the necessary procedures concerning the renewals, she proceeded to take actions immediately. However, by then the interception of the three facilities had already been discontinued. The interception was then resumed after an interruption of about one hour.

6.41 The Team concluded that the incident was caused by the negligence of the duty officer without ulterior motive. The Team proposed to issue a verbal advice (administrative) to the duty officer to advise her to be more vigilant in performing her duty. To prevent recurrence of similar incidents, the Team implemented an alarm system to remind its members including the duty officer and his supervisor to take timely action if a prescribed authorization was to expire on the next working day but instructions for renewal of authorization or discontinuance of facility have not yet been saved in the computer system. I noted the Team's proposed action against the duty officer concerned and the improvement measure.

Case 6.6 : Access to interception products during suspension of monitoring of the interception concerned

6.42 This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.

6.43 In the course of checking the relevant ATR for preparing a notification to be submitted to me in accordance with the COP to report a heightened likelihood of obtaining LPP information from an interception operation, the LEA concerned discovered that an officer, when performing supervisory duties, had listened to five calls during the period when monitoring of the interception concerned should have been put on hold pending submission of an REP-11 report to the panel judge to report the heightened LPP likelihood. When reporting to me the LPP case, the LEA notified me of the incident.

6.44 Subsequently, the LEA submitted an investigation report to me, detailing the results of its investigation into the incident. The investigation by the LEA found that the incident was due to the officer's misunderstanding of the scope of the suspension of monitoring of interception. The officer, who was newly transferred to the interception unit concerned, perceived that during the suspension period, only interception products that involved LPP information or had not been accessed should not be accessed. Hence, she considered that the suspension of monitoring of interception did not apply to re-access to interception products that had already been accessed. In the incident, the monitoring of the interception was suspended and the access right to the interception products concerned was removed after the heightened LPP likelihood was discovered by the LEA. A few days later, due to her misunderstanding of the scope of suspension of monitoring of interception, the officer, despite the suspension of the monitoring of the interception, re-listened to some of the calls which had been listened to by her subordinates previously with a view to performing supervisory check to verify the accuracy of the contents of these calls recorded in the transcripts in respect of the interception operation. As the access right to the interception products was already removed, the officer used a special function of the monitoring system to re-listen to these calls. The special function, which allowed officers to re-listen only to those part(s) of the calls that had been listened to previously, was implemented a few months before to facilitate re-listening to calls with heightened LPP likelihood or LPP information for the purpose of ensuring the accuracy of the contents of these calls to be reported to the panel judge in REP-11 reports. In the incident, a total of five calls were re-listened to by the officer during the suspension of the monitoring of the interception.

6.45 The LEA concluded that there was no foul play or ulterior motive involved in the incident. The sole intent of the officer to re-listen to the five calls in question was to verify the accuracy of the transcripts in respect of these calls which had already been listened to by her

subordinates. The LEA proposed to issue a verbal advice (non-disciplinary) to the officer to remind her to be more cautious in performing interception related duties in future, particularly in the handling of situation where monitoring of interception was suspended. As regards supervisory accountability, the LEA considered that since the officer was a newcomer to the interception unit, her supervisor should have exercised close supervision on her work. The LEA proposed to remind the supervisor of the need to give proper guidance and support to her subordinates, particularly those new to ICSO duties. To prevent recurrence of similar mistakes in future, the LEA tightened up the arrangement for seeking approval of the use of the special function of the monitoring system and enhanced the relevant computer system after the incident.

6.46 In reviewing the case, I listened to the five calls in question and did not find any abnormality. I agreed that there was no foul play or ulterior motive involved in the incident since those five calls had already been listened to by LEA officers and nothing was gained by the officer in re-accessing them. The LEA's proposed actions against the officer and her supervisor as well as the remedial actions taken after the incident were considered appropriate. However, the incident called into question as to whether the officer had been provided with sufficient training on the suspension of monitoring of interception and the use of the special function of the monitoring system. In this connection, I advised the LEA to provide adequate training and guidance to officers before they took up the ICSO duties.

Case 6.7 : Inaccurate information provided in an REP-11 report

6.47 Checking of protected products of a case selected from weekly report revealed that some information provided in the REP-11 report to the panel judge was not accurate. The discrepancies were

related to the information on the usage pattern of two facilities under interception.

6.48 In response to my request for explanations for the discrepancies, the LEA explained that the inaccuracies were due to inadequate attention and lack of caution of two officers in performing the ICSO duties.

6.49 After reviewing the case, I accepted the explanations provided by the LEA. Notwithstanding the discrepancies, I opined that there was no material impact on the validity of the prescribed authorization concerned. Regarding the LEA's proposal that the two officers involved be reminded and be given a verbal advice (non-disciplinary) respectively, I considered them appropriate.

Case 6.8 : Inaccuracy in the recorded time of a covert surveillance product

6.50 An LEA reported an incident where there was a discrepancy between the recorded times of two covert surveillance products.

6.51 A prescribed authorization was granted to the LEA for conducting Type 1 surveillance on two subjects. One day, in preparation for a covert surveillance operation, an officer of the device store ('the Officer') issued through the Device Management System three surveillance devices ('Device A', 'Device B' and 'Device C') to an officer who was assigned as the field command of the operation ('the Field Command Officer').

6.52 During the surveillance operation that was carried out later the same day, Device A and Device C were used simultaneously to record a meeting of the subjects while Device B was not used. After the operation, the Field Command Officer returned the three devices to the device store. On the afternoon of the same day, the Field Command Officer received from

the Officer a copy of the two surveillance products that were obtained through Device A and Device C respectively. During examination of the products, the Field Command Officer found that despite the fact that Device A was switched on later than Device C, the starting time of the recording of Device A was about one minute earlier than that of Device C ('the Discrepancy').

6.53 The LEA subsequently submitted a detailed report to me. According to its operational manual on covert surveillance, the LEA required its officers to synchronise their watches with the Hong Kong Standard Time before conducting covert surveillance, which could be done by making reference to the system clock of the computer network or the master clocks at various offices of the LEA. The LEA informed me that the device store adopted a practice whereby the built-in clocks of the surveillance devices were synchronised with the Hong Kong Standard Time every time before their issue to investigating officers. Officers of the device store should follow such practice by making reference to the master clock at the device store ('the Store's Master Clock'). For Device A, it had to be connected to one of the standalone computers installed with a specific software ('the Designated Computers') for configuration before deployment and its built-in clock could only be synchronised with the clock of any of these Designated Computers during the configuration process.

6.54 With regard to the surveillance operation concerned, the Officer was responsible for synchronising the built-in clocks of Device A and Device B while another officer of the device store was responsible for synchronising the built-in clock of Device C. Both officers made reference to the Store's Master Clock when they synchronised the clocks of Device B and Device C. When synchronising the clock of Device A, the Officer only made reference to his watch. The Officer did not make reference to the Store's Master Clock as he mistakenly believed that the clock of the Designated Computer and his watch, which had been synchronised with the Hong Kong Standard Time before, were precise. It did not occur to

the Officer at the time that the clock of the Designated Computer concerned and his watch might have drifted apart from the Hong Kong Standard Time due to lapse of time. The Officer further explained that the Designated Computer concerned was located at a room ('the Computer Room') where the Store's Master Clock was out of sight. It turned out that there existed a gap of over one minute between the clock of the Designated Computer and the master clock.

6.55 The LEA was of the view that the Discrepancy was attributed to the inadvertence of the Officer who failed to synchronise the built-in clock of Device A with the Hong Kong Standard Time. The LEA recommended that an advice (non-disciplinary) be given to the Officer on the need to be more vigilant in carrying out his duties.

6.56 The LEA had revised its operational manual on covert surveillance to make it clear the requirement for officers of the device store to synchronise the built-in clocks, if any, of the surveillance devices with the Hong Kong Standard Time. The revised operational manual took effect within one month after the incident. Besides, another master clock had been installed at the Computer Room and the clocks of the Designated Computers had been connected to the master clock in order to prevent recurrence of similar incidents.

6.57 I examined the relevant surveillance products and revealed that the two devices recorded the same meeting of the subjects from two different angles. No irregularity was found during the checking.

6.58 I observed that the Officer was aware of the requirement of synchronising the built-in clocks of surveillance devices with the Hong Kong Standard Time. His explanation for not having made reference to the Store's Master Clock when synchronising the clock of Device A was not unreasonable. However, the Discrepancy would have been avoided if he was more vigilant in carrying out his duties. I agreed

with the LEA that the Discrepancy was attributed to the inadvertence of the Officer.

6.59 After reviewing the case, I found no evidence showing that there was any ill intent or ulterior motive involved in the incident since nothing was gained nor was there any loss, the only consequence being a discrepancy of time of about one minute. The recommended action against the Officer was considered acceptable and the improvement measures appropriate.

Case 6.9 : An officer's failure to report to his supervisor a call which might indicate heightened LPP likelihood

6.60 This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.

6.61 At the grant of the prescribed authorization concerned, the interception operation was not assessed to have a likelihood of obtaining LPP information. When checking the protected products, it was found that a call contained information which might indicate heightened LPP likelihood. The LEA concerned was required to clarify whether any assessment of the likelihood of obtaining LPP information arising from the call was made and the assessment result, if any.

6.62 According to the LEA's explanation, the officer concerned, based on her judgement, did not consider the call involved information which indicated heightened LPP likelihood. The LEA concluded that the assessment made by the officer was not unreasonable. Nevertheless, the LEA admitted that the officer had overlooked the requirement of bringing the call to the attention of the supervisor for assessment of the LPP likelihood. The LEA proposed giving a verbal advice (disciplinary) to the officer for not following the internal procedural guideline in performing the monitoring work.

6.63 Having reviewed the case, I considered the explanations provided by the LEA for not considering the call as having information indicating a likelihood of obtaining LPP information acceptable. I agreed that there was no foul play or ulterior motive involved in this case. The LEA's proposed disciplinary action against the officer was considered appropriate.

Case 6.10 : Non-reporting of an earlier call with heightened LPP likelihood

6.64 This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.

6.65 In notifying me of an LPP call, the LEA also reported that there was an earlier 'other call' relating to the Reported LPP Call and this 'other call' did not contain any LPP information or any information indicating heightened LPP likelihood. However, according to the protected products checked, the contents of this earlier 'other call' contained information indicating heightened LPP likelihood. The LEA concerned was requested to advise whether any assessment of the likelihood of obtaining LPP information arising from the call was made and the assessment result, if any. The LEA replied that the officer concerned was not aware of the content of the call which indicated heightened LPP likelihood as her focus was on the relevancy of the content of the call to the investigation. Consequently, the LPP likelihood arising from this call was not assessed and the call was not reported to the panel judge.

6.66 While I accepted the LEA's explanation, I pointed out that had the officer concerned been aware of the heightened LPP likelihood arising from the 'other call' and reported it to the panel judge, it could help minimise the risk of inadvertently obtaining LPP information, if any, in the period between the time the 'other call' was listened to and that of the Reported LPP Call. In light of the case, the LEA had reminded its officers to be more vigilant in performing interception operations under the ICSO.

Case 6.11 : Non-reporting of a call with heightened LPP likelihood

6.67 This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.

6.68 At the grant of the prescribed authorization concerned, the interception operation was assessed to have a likelihood of obtaining LPP information. The interception operation was, therefore, subject to additional conditions imposed by the panel judge to guard against the risk of obtaining LPP information. As the interception progressed, the LEA encountered calls which indicated heightened likelihood of obtaining LPP information. Upon consideration of the REP-11 reports submitted by the LEA, the panel judge allowed the interception to continue.

6.69 One day, an officer of the LEA listened to a call and found that the call contained information which indicated heightened LPP likelihood. The LEA reported the call to the panel judge by way of an REP-11 report and the panel judge allowed the interception to continue with additional conditions imposed. When notifying me of this Reported LPP Call, the LEA reported that there were a certain number of other calls between the telephone number involved in the Reported LPP Call and the subject's telephone number under interception. The LEA mentioned that some of these other calls had been listened to but none of them contained any LPP information or any information indicating heightened LPP likelihood.

6.70 In checking the protected products of this LPP case, I found that one of such other calls, which was intercepted and listened to by the same officer about one week prior to the discovery of the Reported LPP Call, contained information indicating heightened LPP likelihood. I requested the LEA to confirm whether any assessment of the likelihood of obtaining LPP information arising from this earlier call had been made. The LEA replied that the officer was not aware of the phrase in the call which indicated heightened LPP likelihood probably because the content of the call was not relevant to the crime investigation. Consequently, no

assessment on LPP likelihood arising from this call was made and the call was not reported to the panel judge. In its reply, the LEA also informed me that it had advised the officer to adopt a more vigilant approach in carrying out her duties.

6.71 The explanation was considered unacceptable. The phrase indicating heightened LPP likelihood was mentioned in the early part of the call. Despite the fact that the officer may have formed the view that the content of the call was not relevant to the investigation, according to the relevant ATR, she did continue to monitor the call intermittently up to nearly its end.

6.72 I pointed out to the LEA that, even if an intercepted call was not relevant to the investigation, that was no excuse for the officer to relax her vigilance in detecting LPP likelihood. I also emphasised to the LEA that regardless of the relevancy of the contents of the intercepted calls to the investigation, LEA officers should handle all information gathered from interception operations with high vigilance to guard against the risk of obtaining LPP information or JM.

6.73 The officer failed to pick up calls with indication of heightened LPP likelihood despite her having been verbally advised in other incidents of similar nature in 2017. With the repeated failure of the officer, I considered her performance neither satisfactory nor professional. I suggested that the LEA should critically review the suitability of the officer in undertaking interception monitoring duties and take a more effective measure with some degree of deterrence against the officer. After review, the LEA removed the officer from interception monitoring duties and proposed to issue a verbal warning (disciplinary) to her. Having considered the appropriateness and deterrent effect of the proposed action, I accepted the LEA's proposal.

Case 6.12 : An officer's failure to document properly the assessment of the likelihood of obtaining LPP information of a call

6.74 This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4. In checking the protected products of the case, it was noticed that the contents of one 'other call', which appeared before the Reported LPP Call, contained information which might indicate possible heightened LPP likelihood. The LEA concerned was requested to advise whether any assessment of the likelihood of obtaining LPP information arising from the call was made and the assessment result, if any. The LEA replied that the officer concerned was aware of the content of the call which might indicate possible heightened LPP likelihood and reported the issue to his immediate supervisor and the senior supervisor without delay. The LPP likelihood arising from the call was assessed by the senior supervisor. The officer concerned was asked to make written record of the assessment on the relevant document but he failed to do so. The immediate supervisor also failed to note that the officer had not recorded the assessment result on the relevant document when performing his supervisory check.

6.75 The LEA proposed to give a verbal advice (non-disciplinary) each to the officer and the immediate supervisor for reminding them to be more cautious and prudent in performing the ICSO duties. As a remedial measure, the LEA required the supervisor to counter-sign the remark to be made on the relevant document on the assessment result of the likelihood of obtaining LPP information.

6.76 Having reviewed the case, I accepted the LEA's findings that no foul play or ulterior motive was involved since the officer concerned had recorded the full content of the call on the relevant document and reported the matter through proper chain of command for deliberation. The officer's explanation of a genuine lapse of mind leading to the missing of proper documentation of the assessment result was not implausible.

The LEA's proposed disciplinary actions against the two officers concerned and the remedial measure proposed were considered appropriate.

Case 6.13 : Irregularities and non-compliance in a covert surveillance

6.77 A prescribed authorization was granted to an LEA in October 2019 for the conduct of Type 1 surveillance. It was assessed at the time of application that the surveillance operation sought to be authorized would unlikely obtain information subject to LPP. However, the panel judge imposed additional conditions to guard against the risk of obtaining LPP information when he approved the application.

6.78 For cases where LPP information is not involved but additional conditions are imposed on the prescribed authorizations concerned, the LEAs are required to preserve the related protected products and report to me the imposition of the additional conditions through the weekly reports for checking purposes. In this case, the LEA concerned only reported the imposition of the additional conditions to me in December 2019 but not in the relevant weekly report in October 2019.

6.79 In December 2019, the LEA also reported to me an incident that in one of the surveillance operations, a recording lasted about 30 seconds longer than it should. I took the view that these 30 seconds might possibly be outside the ambit of the prescribed authorization such that this surveillance might be a non-compliance with the terms of the prescribed authorization.

6.80 From the checking of the relevant weekly reports and the device register in respect of the prescribed authorization, I observed that a surveillance device which was incompatible with the additional conditions had been issued on three occasions. During a periodical visit, I required the LEA to provide explanations for the delay in reporting the imposition of the additional conditions and the issue of incompatible

surveillance device. The LEA undertook to conduct an investigation and inform me of the outcome.

6.81 The LEA submitted a full investigation report dated 31 March 2020 to me under section 54 of the Ordinance ^{Note 3}. At the time of writing this report, a review on the case is still on-going. Details about my review will be reported in the next annual report.

Other reports

6.82 For the other three cases, they were reports on incidents of technical problems of the computer systems. These cases had been reviewed and nothing untoward was found. The LEAs concerned had also taken appropriate actions to remedy the problems.

Examination of protected products of past cases of non-compliance, irregularity or incident

6.83 For cases of non-compliance, irregularity or incident that did not involve the obtainment of LPP information or JM or such likelihood, depending on the nature of the cases, the Commissioner might request the LEAs to preserve the related protected products for his examination or the LEAs might preserve the related protected products of their own accord for the possible examination by the Commissioner. In the report period, I had selected five such cases including two reported in 2009, two in 2010 and one in 2014 for examination of protected products. Four of these five cases were on covert surveillance while another one was on telecommunications interception. In one of these five cases, my predecessor had mentioned in Annual Report 2010 that conclusion for that case could only be drawn by checking of the recordings. My review after

^{Note 3} The incident report submitted by the LEA in 2019 was not pursuant to section 54 of the Ordinance. After investigation of the incident, the LEA submitted a full investigation report to me in 2020 under section 54 of the Ordinance.

checking of the protected products of this case is detailed in paragraph 6.84 below. The LEA concerned was required to provide explanation for another case and it subsequently submitted a report under section 54 of the Ordinance which is detailed in paragraphs 6.85 to 6.98 below. For the remaining three cases, I did not find anything that deviated from what had been reported to the relevant authority and/or the Commissioner.

Past Case (i) : Type 2 surveillance conducted on an incoming call whose caller was not the subject of the executive authorization [Paragraphs 7.70 to 7.98 of Annual Report 2010]

6.84 A report on a Type 2 surveillance operation conducted on an incoming call, allegedly from a person other than the subject of the executive authorization granted in 2010 was reported in the Annual Report 2010. The then Commissioner, after his review on the incident, had made a comment in paragraph 7.96 of the Annual Report 2010 that the only means to ascertain whether there had been any non-compliance in the case was to listen to the recording of the incoming call. Given the express power to examine the protected products after the enactment of the Interception of Communications and Surveillance (Amendment) Ordinance 2016, I had checked the preserved protected products of this case. I found that the recording device had not captured any voice of the caller in the concerned call and thus, I concluded that there was no non-compliance involved in this case.

Past Case (ii): Type 1 surveillance conducted outside the ambit of the prescribed authorization [Paragraphs 7.162 to 7.225 of Annual Report 2010]

6.85 The case concerned was a Type 1 surveillance with non-compliance reported in the Annual Report 2010.

6.86 This past case involved three surveillance operations. The non-compliance reported in the Annual Report 2010 was on the third operation. After checking the protected products of this past case, I agreed with my predecessor that the third operation was a non-compliance as set out in Annual Report 2010. Notwithstanding this, clarifications were sought from the LEA concerned on the second operation. Upon conducting examination into the case, the LEA reported to me that, pursuant to section 54 of the Ordinance, part of the second operation was conducted outside the ambit of the prescribed authorization concerned.

6.87 The prescribed authorization was granted to the LEA for conducting Type 1 surveillance on meeting(s) between Subject 1 and Subject 2, with or without other person(s) in public place(s).

6.88 The LEA deployed a senior officer to take charge of the Type 1 surveillance and two officers ('Officer A' and 'Officer B') to conduct the field operation. Officer A was briefed by the senior officer on the background of the case and the details of the operational plan. After arriving the meeting place (which is a location accessible to the public) on a specific day, Subjects 1 and 2 were seen meeting with other persons. Officer A then set up the device and started the recording.

6.89 About thirty minutes later, when Subjects 1 and 2 left the meeting place while the other persons still remained there, Officer A and Officer B stayed on to observe and continued the recording.

6.90 After being notified by another team and confirmed that Subjects 1 and 2 were not anticipated to return to the meeting place, Officer A pressed the button of the device to power it off. He immediately reported to the senior officer the conclusion of the operation over the phone but he did not mention the early departure of Subjects 1 and 2 and the continued recording after they had left the meeting place.

6.91 In the evening of that day, Officer A checked the recording and realized that the recording was not able to capture Subjects 1 or 2 or any of the persons attending the meeting at all. He immediately reported the outcome of the recording to the senior officer. The time when Subjects 1 and 2 left the meeting place and the cessation time of recording were recorded in relevant document.

6.92 Officer C, being the officer-in-charge of the investigation, received the documents and recording from Officer A after the operation. She understood from Officer A that the operation had not been successful and the recording contained nothing of evidential value. She had not been aware that the recording in the concerned Type 1 surveillance had continued for ten minutes after the Subjects had left the meeting place.

6.93 In conducting the review of the concerned operation, nothing special was raised by the senior officer when submitting documents for the reviewing officer's ('RO') attention.

6.94 The LEA was of the view that the unauthorized surveillance was attributed to the lack of vigilance and inadequacy in performance in the execution of the operation by Officer A. However, there was no indication of any sinister motive on his part to conceal the absence of subjects from the meeting as he had recorded the fact in relevant document.

6.95 The LEA recommended that a verbal warning (disciplinary) be given to Officer A given the fact that he did not stop the recording upon the subjects leaving the meeting place, resulting in an excessive recording of about ten minutes which was outside the ambit of the prescribed authorization.

6.96 A verbal warning (disciplinary) was proposed to be given to the senior officer for his lack of vigilance as the officer-in-charge of the Type 1 surveillance as he was not alert that the operation might have been conducted outside the ambit of the prescribed authorization. An advice

(non-disciplinary) was proposed to be given to Officer C to remind her of the need to exercise vigilance in reviewing the relevant records of surveillance after receiving them from the field officer. Officer B and the RO had left the LEA and their accounts of the incident could not be obtained.

6.97 As time passed, clear guidelines and more training had been provided to frontline officers responsible for carrying out ICSO duties. Besides, frontline officers involved in surveillance operations were required to record details of what they had reported to the supervisor in respect of the operations within a specified time frame. Such record would also be submitted together with other necessary documents to the reviewing officer(s) for review.

6.98 After reviewing the case, I considered that this was a case of non-compliance. The continuation of surveillance operation on a meeting without the presence of Subjects 1 and 2 did not comply with the terms of the prescribed authorization. However, I found no evidence showing that there was foul play, ulterior motive or deliberate act involved in the unauthorized surveillance. I agreed with the LEA's findings. The recommended actions against the officers involved as well as the improvement measures were considered appropriate.

CHAPTER 7

RECOMMENDATIONS TO HEADS OF LAW ENFORCEMENT AGENCIES

7.1 Section 52(1) of the Ordinance provides that if the Commissioner considers that any arrangements made by any LEA should be changed to better carry out the objects of the Ordinance or the provisions of the COP, the Commissioner may make such recommendations to the head of the LEA as he thinks fit.

7.2 Through discussions with the LEAs during the visits to the LEAs, and the exchange of correspondence with them in the review of their compliance with the relevant requirements of the Ordinance, a number of recommendations were made in the report period to the LEAs to better carry out the objects of the Ordinance. The recommendations made are set out below:

(a) Justifications for not restricting monitoring of interception to officers at a specific rank or above in LPP and JM cases

For LPP and JM cases, officers below a specific rank should not be assigned for the monitoring duties of the interception concerned. If the LEAs propose not to restrict monitoring of the interception concerned to officers at a specific rank or above when making an application for a prescribed authorization or making a report to the panel judge regarding the altered assessment on the likelihood of obtaining LPP information or JM, they should state in the related application or REP-11 report detailed justifications for the panel judge's consideration.

(b) Reporting and preservation requirements for cases where additional conditions are imposed on prescribed authorizations not involving LPP information or JM

For cases involving LPP information or JM, there is already a set of reporting and preservation requirements. For cases where LPP information or JM is not involved but additional conditions are imposed on the prescribed authorizations concerned, the LEAs should preserve the related protected products as if they are LPP or JM cases and report to the Commissioner the imposition of the additional conditions through the weekly reports submitted to him. This will facilitate the Commissioner's checking of the LEAs' compliance with these additional conditions.

(c) Record of assessment on heightened LPP likelihood

In cases where an officer suspects that there may be an indication of heightened LPP likelihood in an intercepted communication but it is later assessed after deliberation by the officer's supervisor that no LPP likelihood is involved, a note should be made in the relevant transcript to record the assessment made.

(d) Reporting of intercepted communications revealing arrest of the subject

If the arrest of the subject is revealed from an intercepted communication, the contents of the communication should also be stated in the section 58 report submitted to the panel judge to report the arrest of the subject.

CHAPTER 8

STATUTORY TABLES

8.1 In accordance with section 49(2) of the Ordinance, this chapter provides separate statistical information in relation to the statutory activities in the report period. The information is set out in table form and comprises the following tables:

- (a) Table 1(a) – interception – number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)];
- (b) Table 1(b) – surveillance – number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)];
- (c) Table 2(a) – interception – major categories of offences for the investigation of which prescribed authorizations have been issued or renewed [section 49(2)(b)(i)];
- (d) Table 2(b) – surveillance – major categories of offences for the investigation of which prescribed authorizations have been issued or renewed [section 49(2)(b)(i)];
- (e) Table 3(a) – interception – number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)];

- (f) Table 3(b) – surveillance – number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)];
- (g) Table 4 – interception and surveillance – number of device retrieval warrants issued and number of applications for the issue of device retrieval warrants refused [section 49(2)(c)(i) and (ii)];
- (h) Table 5 – summary of reviews conducted by the Commissioner under section 41 [section 49(2)(d)(i)];
- (i) Table 6 – number and broad nature of cases of irregularities or errors identified in the reviews [section 49(2)(d)(ii)];
- (j) Table 7 – number of applications for examination that have been received by the Commissioner [section 49(2)(d)(iii)];
- (k) Table 8 – respective numbers of notices given by the Commissioner under section 44(2) and section 44(5) further to examinations [section 49(2)(d)(iv)];
- (l) Table 9 – number of cases in which a notice has been given by the Commissioner under section 48 [section 49(2)(d)(v)];
- (m) Table 10 – broad nature of recommendations made by the Commissioner under sections 50, 51 and 52 [section 49(2)(d)(vi)];
- (n) Table 11 – number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or surveillance carried out pursuant to a prescribed authorization [section 49(2)(d)(vii)]; and

- (o) Table 12 – number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 42, 47, 52 or 54 and the broad nature of such action [section 49(2)(d)(viii)].

Table 1(a)

Interception – Number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)]

		Judge's Authorization	Emergency Authorization
(i)	Number of authorizations issued	631	0
	Average duration	30 days	—
(ii)	Number of authorizations renewed	679	Not applicable
	Average duration of renewals	30 days	—
(iii)	Number of authorizations issued as a result of an oral application	0	0
	Average duration	—	—
(iv)	Number of authorizations renewed as a result of an oral application	0	Not applicable
	Average duration of renewals	—	—
(v)	Number of authorizations that have been renewed during the report period further to 5 or more previous renewals	12	Not applicable
(vi)	Number of applications for the issue of authorizations refused	4	0
(vii)	Number of applications for the renewal of authorizations refused	0	Not applicable
(viii)	Number of oral applications for the issue of authorizations refused	0	0
(ix)	Number of oral applications for the renewal of authorizations refused	0	Not applicable

Table 1(b)

Surveillance – Number of authorizations issued/renewed with the average duration of the respective authorizations and number of applications refused [section 49(2)(a)]

		Judge's Authorization	Executive Authorization	Emergency Authorization
(i)	Number of authorizations issued	17	3	0
	Average duration	15 days	7 days	—
(ii)	Number of authorizations renewed	5	0	Not applicable
	Average duration of renewals	23 days	—	—
(iii)	Number of authorizations issued as a result of an oral application	0	0	0
	Average duration	—	—	—
(iv)	Number of authorizations renewed as a result of an oral application	0	0	Not applicable
	Average duration of renewals	—	—	—
(v)	Number of authorizations that have been renewed during the report period further to 5 or more previous renewals	0	0	Not applicable
(vi)	Number of applications for the issue of authorizations refused	0	0	0
(vii)	Number of applications for the renewal of authorizations refused	0	0	Not applicable
(viii)	Number of oral applications for the issue of authorizations refused	0	0	0
(ix)	Number of oral applications for the renewal of authorizations refused	0	0	Not applicable

Table 2(a)

**Interception – Major categories of offences for the investigation of which prescribed authorizations have been issued or renewed
[section 49(2)(b)(i)]**

Offence	Chapter No. of Laws of Hong Kong	Ordinance and Section
Trafficking in dangerous drug	Cap. 134	Section 4, Dangerous Drugs Ordinance
Bookmaking	Cap. 148	Section 7, Gambling Ordinance
Making or possession of explosive	Cap. 200	Section 55, Crimes Ordinance
Destroying or damaging property	Cap. 200	Section 60, Crimes Ordinance
Offering advantage to public servant and accepting advantage by public servant	Cap. 201	Section 4, Prevention of Bribery Ordinance
Agent accepting advantage and offering advantage to agent	Cap. 201	Section 9, Prevention of Bribery Ordinance
Robbery	Cap. 210	Section 10, Theft Ordinance
Burglary	Cap. 210	Section 11, Theft Ordinance
Conspiracy to inflict grievous bodily harm/shooting with intent/wounding with intent	Cap. 212	Section 17, Offences against the Person Ordinance
Dealing with property known or believed to represent proceeds of indictable offence	Cap. 455	Section 25, Organized and Serious Crimes Ordinance

Table 2(b)

**Surveillance – Major categories of offences for the investigation of
which prescribed authorizations have been issued or renewed
[section 49(2)(b)(i)]**

Offence	Chapter No. of Laws of Hong Kong	Ordinance and Section
Trafficking in dangerous drug	Cap. 134	Section 4, Dangerous Drugs Ordinance
Bookmaking	Cap. 148	Section 7, Gambling Ordinance
Offering advantage to public servant and accepting advantage by public servant	Cap. 201	Section 4, Prevention of Bribery Ordinance
Agent accepting advantage and offering advantage to agent	Cap. 201	Section 9, Prevention of Bribery Ordinance

Table 3(a)

Interception – Number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]

	Number of persons arrested ^{Note 4}		
	Subject	Non-subject	Total
Interception	120	169	289

Table 3(b)

Surveillance – Number of persons arrested as a result of or further to any operation carried out pursuant to a prescribed authorization [section 49(2)(b)(ii)]

	Number of persons arrested ^{Note 5}		
	Subject	Non-subject	Total
Surveillance	49	16	65

^{Note 4} Of the 289 persons arrested, 38 were attributable to both interception and surveillance operations that had been carried out.

^{Note 5} Of the 65 persons arrested, 38 were attributable to both interception and surveillance operations that had been carried out. The total number of persons arrested under all statutory activities was in fact 316.

Table 4

Interception and surveillance – Number of device retrieval warrants issued and number of applications for the issue of device retrieval warrants refused [section 49(2)(c)(i) & (ii)]

(i)	Number of device retrieval warrants issued	0
	Average duration	–
(ii)	Number of applications for device retrieval warrants refused	0

Table 5

**Summary of reviews conducted by the Commissioner under section 41
[section 49(2)(d)(i)]**

Section 41(1)

Reviews on compliance by departments and their officers with relevant requirements, as the Commissioner considers necessary

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
(a) Regular reviews on weekly reports	208	Interception & Surveillance	LEAs are required to submit weekly reports to the Secretariat providing relevant information on authorizations obtained, applications refused and operations discontinued in the preceding week, for checking and review purposes. During the report period, a total of 208 weekly reports were submitted by the LEAs.
(b) Periodical visits to LEAs	36	Interception & Surveillance	During the report period, 36 visits were made to the LEAs for detailed checking of the application files of doubtful cases as identified from the weekly reports. Moreover, random inspection of other cases and checking of surveillance devices would also be made during the visits. Whenever he considered necessary, the Commissioner would seek clarification or explanation from LEAs directly. From the said visits, a total of 930 applications and 832 related documents/matters had been checked. (See paragraph 2.23 of Chapter 2 and paragraphs 3.22 and 3.23 of Chapter 3.)
(c) Examination of protected products at the LEAs' offices	49	Interception & Surveillance	In 2019, 49 visits were made to the LEAs for examination of protected products. Specific cases such as LPP and JM cases reported by the LEAs, interception products of

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>427 authorizations and surveillance products of six selected authorizations were examined.</p> <p>(See paragraph 2.26 of Chapter 2 and paragraph 3.28 of Chapter 3.)</p>
(d) LPP cases reviewed by the Commissioner	184	Interception & Surveillance (29 reviews)	<p><u>Outstanding LPP cases in 2018</u> 29 cases of heightened LPP likelihood were still on-going beyond 2018 and the authorized operations of these cases were discontinued in 2019.</p> <p>The review of these cases had been completed. Other than one case which involved an incident of technical problem of the computer system mentioned in paragraph 6.130 of Annual Report 2018 and another case which was related to the incident referred to in Case 6.3 of Chapter 6, nothing untoward was revealed.</p> <p>(See paragraph 4.8 of Chapter 4.)</p>
		Surveillance	<p><u>One case of obtaining information suspected to be subject to LPP</u> At the grant of a prescribed authorization for Type 1 surveillance, the operation concerned was assessed to have a likelihood of obtaining LPP information. The panel judge imposed additional conditions on the prescribed authorization to guard against the risk of obtaining LPP information.</p> <p>On one day, surveillance was conducted on a meeting. Shortly after the meeting, the crime investigation was turned overt and the LEA discontinued the Type 1 surveillance. Later the same day, the surveillance products obtained from the meeting were handed over to the dedicated unit for screening.</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>From the screening on one of the surveillance products, an officer of the dedicated unit found that at the last few minutes of the meeting, the subject said something which contained information that was suspected to be subject to LPP. The LEA submitted to the panel judge an REP-11 report and a discontinuance report. The panel judge noted the REP-11 report and duly revoked the prescribed authorization. A similar notification with a copy of the REP-11 report and the discontinuance report was submitted to the Commissioner.</p> <p>The Commissioner reviewed the case and did not find any irregularities. As regards the information suspected to be subject to LPP, the Commissioner examined the recording and considered that LPP information had been inadvertently obtained. The record stated in the REP-11 report was correct. The Commissioner also checked and confirmed that the information passed on to the investigators did not contain any information subject to LPP that should have been screened out.</p> <p>(See paragraphs 4.14 to 4.17 of Chapter 4.)</p>
	Interception & Surveillance (154 reviews)	<p><u>139 cases of heightened LPP likelihood and 15 cases of assessed LPP likelihood</u></p> <p>All the relevant documents and records were checked and the protected products were examined. Except for the eight LPP cases mentioned in Cases 6.4, 6.5 (involved two LPP cases), 6.6, 6.9, 6.10, 6.11 and 6.12, and one case involved an incident of technical problem of the computer systems mentioned in</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>paragraph 6.82 of Chapter 6, nothing untoward was found.</p> <p>(See paragraph 4.18 of Chapter 4.)</p>
(e) JM cases reviewed by the Commissioner	5	Interception	<p><u>Five cases of heightened JM likelihood</u> The relevant documents, records and protected products of the five heightened JM likelihood cases were checked and nothing untoward was found.</p> <p>(See paragraphs 4.22 to 4.24 of Chapter 4.)</p>
(f) Examination of protected products of past LPP cases that were reported before 2016	6	Interception & Surveillance	<p><u>Six past cases</u> The preserved protected products for six cases were checked and nothing untoward was found.</p> <p>(See paragraph 4.25 of Chapter 4.)</p>
(g) Non-compliance/irregularities/incidents reviewed by the Commissioner	17	Surveillance	<p><u>Outstanding case (ii)</u> The case concerned was a Type 1 surveillance which took place in 2018.</p> <p>A prescribed authorization was applied for by the LEA concerned to conduct Type 1 surveillance on a subject. In granting the authorization, the panel judge required the subject to be present in the specified premises when the surveillance was carried out</p> <p>The Divisional Head in charge of the operation ('Officer A') of the LEA wrongly interpreted the term and failed to make operational arrangement to ensure compliance with the term.</p> <p>During the examination of the relevant documents and protected products, the Commissioner observed that there were occasions where surveillance was conducted</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>when the subject was not present in the specified premises, which was not in compliance with the term of the prescribed authorization. The Commissioner requested the LEA to give a full account on the arrangement in conducting the surveillance operation.</p> <p>The LEA stated in the investigation report that at certain periods of the surveillance operation conducted, the subject was not inside the specified premises.</p> <p>The LEA commented that Officer A was not aware of any potential non-compliance in the operation prior to the observation made by the Commissioner. There was no evidence of any wilful or deliberate breach of the term, or any attempt of concealment of such non-compliance. In the reviewing process of this surveillance operation, the two senior officers ('Senior Officer B' and 'Senior Officer C') involved were in acting capacities at the material time. The LEA pointed out that both of them were not familiar with the surveillance duties. Due to lack of experience in surveillance operations, they failed to detect the non-compliance in the reviewing process.</p> <p>The LEA proposed to give a verbal warning (disciplinary) to Officer A, and a verbal advice (disciplinary) each to Senior Officer B and Senior Officer C.</p> <p>The Commissioner had reviewed the case. The misinterpretation of the term of the prescribed authorization by Officer A consequentially affected the execution arrangement of the surveillance operation. The lack of</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>adequate and proper arrangement in ensuring that the subject was inside the specified premises when the surveillance operation took place led to possible situation of non-compliance.</p> <p>There was one period of unauthorized surveillance supported by evidence. There were also several periods of suspected non-compliance which could not be further verified.</p> <p>While the Commissioner had no objection to the comment in the investigation report that there was no evidence to suggest any concealment of the unauthorized surveillance by any of the officers concerned, the Commissioner considered the reviewing process of the surveillance operation conducted by Senior Officers B and C undesirable and disappointing. The mistakes made were left unnoticed even after going through two levels of review. One major reason was that both reviewing officers were in acting capacities at the material time and were not familiar with the covert surveillance duties. It was unsatisfactory that during the reviewing process, Senior Officers B and C only went through the doubtful areas with Officer A without seeking additional advices/views from the relevant team.</p> <p>The Commissioner considered the proposed disciplinary action against Officer A too lenient and requested the LEA to review it while the proposed disciplinary actions against Senior Officer B and Senior Officer C were considered proportionate. After review, the LEA proposed that on top of a verbal warning</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>(disciplinary), Officer A would also be removed from ICSO related duties. Having considered the appropriateness and deterrent effect of the proposed action, the Commissioner accepted the LEA's proposal.</p> <p>As a remedial measure, the LEA proposed enhanced training on the related surveillance topic to all officers in the relevant units and training on ICSO related duties be extended to officers who would have a role to play in the ICSO regime when acting up. Officers in acting capacities who were required to discharge ICSO functions were reminded to seek assistance in case of any doubt. The Commissioner considered the proposed measures appropriate and necessary.</p> <p>(See paragraphs 6.7 to 6.18 of Chapter 6.)</p>
	Interception	<p><u>Case 6.1</u> The non-compliance in this case was discovered by the Commissioner in early 2019 during review of a case of heightened likelihood of obtaining LPP information referred to in Chapter 4 of Annual Report 2018.</p> <p>At the grant of the prescribed authorization concerned, the interception operation was not assessed to have a likelihood of obtaining LPP information. As the interception progressed, one day, an officer of the LEA concerned listened to part of a call and found that the call contained information which indicated heightened LPP likelihood. The panel judge, having considered the REP-11 report submitted by the LEA, allowed the prescribed authorization to continue with</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>additional conditions imposed to guard against the risk of obtaining LPP information. One of the additional conditions was that officers of the LEA should refrain from accessing interception products involving a specified telephone number ('the prohibited number'). In order to comply with this additional condition, the LEA input the prohibited number into the relevant computer system, which would debar officers from accessing all the interception products involving the prohibited number.</p> <p>The Commissioner found that, after the imposition of the additional conditions, one call involving the prohibited number was listened to by an officer for two seconds. It was a breach of the additional condition mentioned above. The Commissioner requested the LEA to conduct an investigation.</p> <p>The investigation by the LEA found that the incident was due to a system bug, resulting in the failure of the computer system to screen out all the interception products involving the prohibited number under certain circumstances. As the computer system had always been very reliable, the officer concerned did not expect the malfunction of the computer system and listened to the call inadvertently. In this regard, the LEA considered that the officer should not be held responsible for the incident and proposed not to take any disciplinary action against the officer. To prevent recurrence of similar incidents, immediate actions were taken to resolve the computer problem.</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>In reviewing the case, the Commissioner listened to the call in question, which confirmed that it did not contain any information subject to LPP or information indicating heightened LPP likelihood. The Commissioner noted the LEA's findings and considered the proposal of not taking any disciplinary action against the officer acceptable.</p> <p>(See paragraphs 6.20 to 6.24 of Chapter 6.)</p>
	Interception	<p><u>Case 6.2</u></p> <p>An LEA reported to the Commissioner an incident where the user identity stated in the ATRs in respect of monitoring of interception by an officer was incorrect.</p> <p>To carry out monitoring of interception, officers of the LEA are required to use their access cards to log in the relevant monitoring systems. One day, an officer ('Officer A') found that her access card malfunctioned. The card was, therefore, sent to another officer ('Officer B') for resetting. In resetting the access card of Officer A, Officer B wrongly selected the user identity of another officer from a list of users and assigned it to Officer A's access card. After the access card was reset, Officer A used it to log in a system to conduct monitoring of interception but she did not notice that the user identity was not hers. A few hours later, Officer A logged in again to conduct monitoring of interception and discovered the mistake. She reported the matter to her supervisor immediately. As a result of the mistake, the user identity shown in the ATRs in respect of the monitoring of interception by</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>Officer A for the period concerned was wrong.</p> <p>The investigation by the LEA concluded that no bad faith or ulterior motive was involved in the incident. The LEA proposed that both Officer A and Officer B be verbally advised (non-disciplinary). To prevent recurrence of similar incidents, an enhancement measure was implemented in the computer system concerned.</p> <p>Having reviewed the case, the Commissioner agreed that no bad faith or ulterior motive was involved in the incident since there was nothing to be gained by Officer B in wrongly selecting the user identity of Officer A. The Commissioner considered the action taken against the two officers concerned as well as the enhancement measure in the computer system appropriate.</p> <p>(See paragraphs 6.25 to 6.28 of Chapter 6.)</p>
		Interception	<p><u>Case 6.3</u></p> <p>The non-compliance was related to a case of heightened likelihood of obtaining LPP information mentioned in paragraph 4.8 of Chapter 4.</p> <p>At the grant of the prescribed authorization, the identity of the subject was already known by the LEA concerned. As the interception progressed, one day, an LEA officer listened to a call, which revealed an alias of the subject ('the first alias'). The officer reported such to his supervisor, who undertook to report this newly surfaced alias to the panel judge as a material change in the circumstances. However, the supervisor forgot to do so.</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>Several months later, another alias of the subject ('the second alias') was revealed in a message intercepted. Having been informed of such, the supervisor reviewed the relevant transcripts for preparation of an REP-11 report to report on the second alias. During the review of the transcripts, the supervisor noted that the first alias was mentioned in a transcript. He then recalled that he had forgotten to submit an REP-11 report to the panel judge to report on the first alias. The supervisor reported the matter to his senior immediately. Subsequently, an REP-11 report was submitted to the panel judge to report on the two aliases of the subject. The LEA reported the matter to the Commissioner.</p> <p>The investigation by the LEA concluded that the delay in reporting the first alias was due to a momentary lapse of mind of the supervisor and there was no foul play or ulterior motive involved. The LEA proposed to give a verbal advice (disciplinary) to the supervisor for his lack of vigilance in making a timely report to the panel judge. To prevent recurrence of similar incidents, the LEA strengthened the procedures for the reporting of the identity or alias of the subject.</p> <p>As required under section 58A of the Ordinance and paragraph 116 of the COP, the reporting of an alias of the subject should be made as soon as reasonably practicable. In this case, the first alias was reported to the panel judge several months after it surfaced. This was a non-compliance with the provision of the Ordinance and the COP.</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>Having reviewed the case, the Commissioner agreed that no foul play or ulterior motive was involved in the delay in reporting the first alias since the full identity of the subject was already known to the LEA at the outset and so nothing was to be gained by the delay in reporting the alias. The proposed disciplinary action against the supervisor and the revised procedures for the reporting of the identity or alias of the subject were considered appropriate.</p> <p>(See paragraphs 6.29 to 6.33 of Chapter 6.)</p>
		Interception	<p><u>Case 6.4</u> An LEA reported to the Commissioner an incident of delay in reporting to the panel judge on the previous arrest of the subject. This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>Two prescribed authorizations were granted respectively for interception on two subjects, whose identities were not known to the LEA at the time of applying for the authorizations. As the interception progressed, one day, the LEA learnt of the identities of the two subjects and found that they were the same person. Having checked the relevant computer record, the investigation team of the LEA did not find any outstanding case in respect of any arrest of the subject and informed the interception unit of the checking result accordingly. Two days later, the interception unit submitted REP-11 reports to the panel judge to report the identity of the subject. Later on the same day, when reviewing the relevant investigation documents, a senior</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>officer of the investigation team found that the subject was, indeed, being on bail in connection with his arrest which happened about one month before. The arrest was unrelated to the offence for which the interception operations were authorized. Subsequently, the LEA submitted to the panel judge section 58 reports to report the arrest status of the subject and REP-11 reports to report the non-reporting of the subject's arrest status in the REP-11 reports submitted before. The panel judge allowed the authorizations to continue with additional conditions imposed to guard against the risk of obtaining LPP information.</p> <p>The investigation by the LEA found that the incident was mainly due to the carelessness of an officer. The officer reported the wrong checking result to her supervisor verbally. The supervisor, without counter-checking the relevant investigation record, submitted a written report via the senior officer (who discovered the mistake two days later) to the interception unit that the subject had no outstanding case. As a result, no section 58 report was submitted by the interception unit to report the arrest status of the subject at the same time when the identity of the subject was reported to the panel judge.</p> <p>The LEA concluded that no foul play or ulterior motive was involved in the incident. The LEA proposed to give a verbal warning (disciplinary) to the officer and the supervisor for their carelessness or oversight. The LEA also proposed to give a verbal advice (disciplinary) to the senior officer given his supervisory accountability.</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>The Commissioner have reviewed the case. There was no evidence to contradict the findings of the LEA that there was no foul play or ulterior motive involved in the incident. The proposed disciplinary actions against the officers concerned were considered appropriate.</p> <p>(See paragraphs 6.34 to 6.38 of Chapter 6.)</p>
	Interception	<p><u>Case 6.5</u></p> <p>The interception of telecommunications facilities by an LEA is made through a dedicated team ('the Team') which operates independently of the investigative arms of the LEAs. The Team reported to the Commissioner an incident in which the telecommunications interception of three facilities was inadvertently discontinued due to a human error. Two cases of heightened likelihood of obtaining LPP information referred to in Chapter 4 were involved in the incident.</p> <p>The renewal of prescribed authorizations for the interception of the three facilities was granted by the panel judge on the day before the authorizations were to expire. The LEA concerned then passed the relevant documents to the Team. The Team was required to input details of the renewals to the relevant computer system on the same day or otherwise the interception would be discontinued automatically. However, upon receiving the relevant documents from the LEA, the duty officer of the Team failed to process the renewals on the computer system on that day. On the next day, when the duty officer recalled that she had not performed the necessary</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>procedures concerning the renewals, she proceeded to take actions immediately. However, by then the interception of the three facilities had already been discontinued. The interception was then resumed after an interruption of about one hour.</p> <p>The Team concluded that the incident was caused by the negligence of the duty officer without ulterior motive. The Team proposed to issue a verbal advice (administrative) to the duty officer. To prevent recurrence of similar incidents, the Team implemented an alarm system to remind its members to take timely action if a prescribed authorization was to expire on the next working day but instructions for renewal of authorization or discontinuance of facility have not yet been saved in the computer system. The Commissioner noted the Team's proposed action against the duty officer and the improvement measure.</p> <p>(See paragraphs 6.39 to 6.41 of Chapter 6.)</p>
	Interception	<p><u>Case 6.6</u> This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>In the course of checking the relevant ATR for preparing a notification to be submitted to the Commissioner in accordance with the COP to report a heightened likelihood of obtaining LPP information from an interception operation, the LEA concerned discovered that an officer, when performing supervisory duties, had listened to five calls during the period when monitoring of the interception concerned should have been put on</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>hold pending submission of an REP-11 report to the panel judge.</p> <p>The LEA submitted a report to the Commissioner detailing the results of its investigation into the incident. The LEA found that the incident was due to the officer's misunderstanding of the scope of the suspension of monitoring of interception. The officer, who was newly transferred to the interception unit concerned, perceived that during the suspension period, only interception products that involved LPP information or had not been accessed should not be accessed. Hence, she considered that the suspension of monitoring of interception did not apply to re-access of interception products that had already been accessed. In the incident, the monitoring of the interception was suspended and the access right to the interception products concerned was removed after the heightened LPP likelihood was discovered by the LEA. A few days later, the officer, despite the suspension of the monitoring of the interception, re-listened to some of the calls which had been listened to by her subordinates previously with a view to verifying the accuracy of the contents of these calls recorded in the transcripts. As the access right to the interception products was already removed, the officer used a special function of the monitoring system to re-listen to these calls. The special function, which allowed officers to re-listen only to those part(s) of the calls that had been listened to previously, was implemented to facilitate re-listening to calls with heightened LPP likelihood or LPP information for the purpose of ensuring the accuracy of the contents of these calls to be</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>reported to the panel judge in REP-11 reports. In the incident, a total of five calls were re-listened to by the officer during the suspension of the monitoring of the interception.</p> <p>The LEA concluded that there was no foul play or ulterior motive involved in the incident. The sole intent of the officer was to verify the accuracy of the transcripts in respect of these calls which had already been listened to by her subordinates. The LEA proposed to issue a verbal advice (non-disciplinary) to the officer to remind her to be more cautious in performing interception related duties in future. The LEA considered that since the officer was a newcomer to the interception unit, her supervisor should have exercised close supervision on her work. The LEA proposed to remind the supervisor of the need to give proper guidance and support to her subordinates. To prevent recurrence of similar mistakes in future, the LEA tightened up the arrangement for seeking approval of the use of the special function of the monitoring system and enhanced the relevant computer system.</p> <p>In reviewing the case, the Commissioner listened to the five calls in question and did not find any abnormality. The Commissioner agreed that there was no foul play or ulterior motive involved in the incident since those five calls had already been listened to by LEA officers. The LEA's proposed actions against the officer and her supervisor as well as the remedial actions taken after the incident were considered appropriate.</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>The incident called into question as to whether the officer had been provided with sufficient training on the suspension of monitoring of interception and the use of the special function of the monitoring system. In this connection, the Commissioner advised the LEA to provide adequate training and guidance to officers before they took up the ICSO duties.</p> <p>(See paragraphs 6.42 to 6.46 of Chapter 6.)</p>
	Interception	<p><u>Case 6.7</u> Checking of protected products of a case revealed that some information provided in the REP-11 report to the panel judge was not accurate.</p> <p>In response to the Commissioner's request for explanations for the discrepancies, the LEA explained that the inaccuracies were due to inadequate attention and lack of caution of two officers in performing the ICSO duties.</p> <p>After reviewing the case, the Commissioner accepted the explanations provided by the LEA. Notwithstanding the discrepancies, the Commissioner opined that there was no material impact on the validity of the prescribed authorization concerned. The Commissioner considered the LEA's proposal that one officer be reminded and the other officer be given a verbal advice (non-disciplinary) appropriate.</p> <p>(See paragraphs 6.47 to 6.49 of Chapter 6.)</p>
	Surveillance	<p><u>Case 6.8</u> An LEA reported an incident where there was a discrepancy between the</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>recorded times of two covert surveillance products.</p> <p>A prescribed authorization was granted to the LEA for conducting Type 1 surveillance. One day, in preparation for a covert surveillance operation, an officer of the device store ('the Officer') issued three surveillance devices ('Device A', 'Device B' and 'Device C') to an officer who was assigned as the field command of the operation ('the Field Command Officer').</p> <p>During the surveillance operation that was carried out later the same day, Device A and Device C were used simultaneously to record a meeting of the subjects while Device B was not used. After the operation, the Field Command Officer returned the three devices to the device store. The Field Command Officer found that despite the fact that Device A was switched on later than Device C, the starting time of the recording of Device A was about one minute earlier than that of Device C ('the Discrepancy').</p> <p>The LEA subsequently submitted a detailed report to the Commissioner. According to its operational manual on covert surveillance, the LEA required its officers to synchronise their watches with the Hong Kong Standard Time before conducting covert surveillance, which could be done by making reference to the system clock of the computer network or the master clocks at various offices of the LEA. The device store adopted a practice whereby the built-in clocks of the surveillance devices were synchronised with the Hong Kong Standard Time every time before</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>their issue to investigating officers. Officers of the device store should follow such practice by making reference to the master clock at the device store ('the Store's Master Clock'). For Device A, it had to be connected to one of the standalone computers installed with a specific software ('the Designated Computers') for configuration before deployment and its built-in clock could only be synchronised with the clock of any of these Designated Computers during the configuration process.</p> <p>With regard to the surveillance operation concerned, the Officer was responsible for synchronising the built-in clocks of Device A and Device B while another officer of the device store was responsible for synchronising the built-in clock of Device C. Both officers made reference to the Store's Master Clock when they synchronised the clocks of Device B and Device C. When synchronising the clock of Device A, the Officer only made reference to his watch. He did not make reference to the Store's Master Clock as he mistakenly believed that the clock of the Designated Computer and his watch were precise. The Officer further explained that the Designated Computer concerned was located at a room ('the Computer Room') where the Store's Master Clock was out of sight. It turned out that there existed a gap of over one minute between the clock of the Designated Computer and the master clock.</p> <p>The LEA was of the view that the Discrepancy was attributed to the inadvertence of the Officer who failed to synchronise the built-in clock of Device A with the Hong Kong</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>Standard Time. The LEA recommended that an advice (non-disciplinary) be given to the Officer.</p> <p>The LEA had revised its operational manual on covert surveillance to make it clear the requirement for officers of the device store to synchronise the built-in clocks, if any, of the surveillance devices with the Hong Kong Standard Time. Besides, another master clock had been installed at the Computer Room and the clocks of the Designated Computers had been connected to the master clock in order to prevent recurrence of similar incidents.</p> <p>The Commissioner examined the relevant surveillance products and revealed that the two devices recorded the same meeting of the subjects from two different angles. No irregularity was found during the checking.</p> <p>The Commissioner observed that the Officer was aware of the requirement of synchronising the built-in clocks of surveillance devices with the Hong Kong Standard Time. His explanation for not having made reference to the Store's Master Clock when synchronising the clock of Device A was not unreasonable. However, the Discrepancy would have been avoided if he was more vigilant in carrying out his duties. The Commissioner agreed with the LEA that the Discrepancy was attributed to the inadvertence of the Officer.</p> <p>After reviewing the case, the Commissioner found no evidence showing that there was any ill intent or ulterior motive involved in the incident since nothing was gained nor</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>was there any loss, the only consequence being a discrepancy of time of about one minute. The Commissioner considered the recommended action against the Officer acceptable and the improvement measures appropriate.</p> <p>(See paragraphs 6.50 to 6.59 of Chapter 6.)</p>
	Interception	<p><u>Case 6.9</u> This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>At the grant of the prescribed authorization concerned, the interception operation was not assessed to have a likelihood of obtaining LPP information. In checking the protected products, it was found that a call contained information which might indicate heightened LPP likelihood. The LEA concerned was required to clarify whether any assessment of the likelihood of obtaining LPP information arising from the call was made and the assessment result, if any.</p> <p>According to the LEA's explanation, the officer concerned, based on her judgement, did not consider the call involved information which indicated heightened LPP likelihood. The LEA concluded that the assessment made by the officer was not unreasonable. Nevertheless, the LEA admitted that the officer had overlooked the requirement of bringing the call to the attention of the supervisor for assessment of the LPP likelihood. The LEA proposed giving a verbal advice (disciplinary) to the officer for</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>not following the internal procedural guideline in performing the monitoring work.</p> <p>Having reviewed the case, the Commissioner considered the explanations provided by the LEA acceptable. The Commissioner agreed that there was no foul play or ulterior motive involved in this case. The LEA's proposed disciplinary action against the officer was considered appropriate.</p> <p>(See paragraphs 6.60 to 6.63 of Chapter 6.)</p>
	Interception	<p><u>Case 6.10</u></p> <p>This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>In notifying the Commissioner of an LPP call, the LEA also reported that there was an earlier 'other call' relating to the Reported LPP Call and this 'other call' did not contain any LPP information or any information indicating heightened LPP likelihood. However, according to the protected products checked, the contents of this earlier 'other call' contained information indicating heightened LPP likelihood. The LEA was requested to clarify whether any assessment of the likelihood of obtaining LPP information arising from the call was made and the assessment result, if any. The LEA replied that the officer concerned was not aware of the content of the call which indicated heightened LPP likelihood as her focus was on the relevancy of the content of the call to the investigation. Consequently, the LPP likelihood arising from this call</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>was not assessed and the call was not reported to the panel judge.</p> <p>While the Commissioner accepted the LEA's explanation, he pointed out that had the officer concerned been aware of the heightened LPP likelihood arising from the 'other call' and reported it to the panel judge, it could help minimise the risk of inadvertently obtaining LPP information, if any, in the period between the time the 'other call' was listened to and that of the Reported LPP Call. The LEA had reminded its officers to be more vigilant in performing interception operations under the ICSO.</p> <p>(See paragraphs 6.64 to 6.66 of Chapter 6.)</p>
	Interception	<p><u>Case 6.11</u></p> <p>This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>At the grant of the prescribed authorization concerned, the interception operation was assessed to have a likelihood of obtaining LPP information. The interception operation was, therefore, subject to additional conditions imposed by the panel judge to guard against the risk of obtaining LPP information.</p> <p>One day, an officer of the LEA listened to a call and found that the call contained information which indicated heightened LPP likelihood. The LEA reported the call to the panel judge by way of an REP 11 report and the panel judge allowed the interception to continue with additional conditions imposed. When notifying the Commissioner of</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>this Reported LPP Call, the LEA reported that there were a certain number of other calls between the telephone number involved in the Reported LPP Call and the subject's telephone number under interception.</p> <p>In checking the protected products of this LPP case, the Commissioner found that one of such other calls, which was listened to by the same officer, contained information indicating heightened LPP likelihood. The LEA explained that the officer was not aware of the phrase in the call which indicated heightened LPP likelihood probably because the content of the call was not relevant to the crime investigation. Consequently, no assessment on LPP likelihood arising from this call was made and the call was not reported to the panel judge.</p> <p>The explanation was considered unacceptable. The phrase indicating heightened LPP likelihood was mentioned in the early part of the call. Despite the fact that the officer may have formed the view that the content of the call was not relevant to the investigation, according to the relevant ATR, she did continue to monitor the call intermittently up to nearly its end.</p> <p>The Commissioner pointed out to the LEA that, even if an intercepted call was not relevant to the investigation, that was no excuse for the officer to relax her vigilance in detecting LPP likelihood. The Commissioner also emphasised to the LEA that regardless of the relevancy of the contents of the intercepted calls to the investigation, LEA officers should handle all information gathered from</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>interception operations with high vigilance to guard against the risk of obtaining LPP information or JM.</p> <p>The officer failed to pick up calls with indication of heightened LPP likelihood despite her having been verbally advised in other incidents of similar nature in 2017. With the repeated failure of the officer, the Commissioner considered her performance neither satisfactory nor professional. The Commissioner suggested that the LEA should critically review the suitability of the officer in undertaking interception monitoring duties and take a more effective measure with some degree of deterrence against the officer. After review, the LEA removed the officer from interception monitoring duties and proposed to issue a verbal warning (disciplinary) to her. Having considered the appropriateness and deterrent effect of the proposed action, the Commissioner accepted the LEA's proposal.</p> <p>(See paragraphs 6.67 to 6.73 of Chapter 6.)</p>
		Interception	<p><u>Case 6.12</u></p> <p>This incident was related to a case of heightened likelihood of obtaining LPP information referred to in Chapter 4.</p> <p>In checking the protected products of the case, it was noticed that the contents of an 'other call' contained information which might indicate possible heightened LPP likelihood.</p> <p>Upon enquiry, the LEA replied that the officer concerned was aware of the content of the call which might</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>indicate possible heightened LPP likelihood and had reported the issue to his immediate supervisor and the senior supervisor without delay. The LPP likelihood arising from the call was assessed by the senior supervisor. The officer was asked to make written record of the assessment on the relevant document but he failed to do so. The immediate supervisor also failed to note that the officer had not recorded the assessment result on the relevant document when performing his supervisory check.</p> <p>The LEA proposed to give a verbal advice (non-disciplinary) each to the officer and the immediate supervisor, reminding them to be more cautious and prudent in performing ICSO duties. As a remedial measure, the LEA required the supervisor to counter-sign the remark to be made on the relevant document on the assessment of the likelihood of obtaining LPP information.</p> <p>Having reviewed the case, the Commissioner accepted the LEA's findings that no foul play or ulterior motive was involved since the officer concerned had recorded the full content of the call on the relevant document and reported the matter through proper chain of command for deliberation. The officer's explanation of a genuine lapse of mind leading to the missing of proper documentation of the assessment result was not implausible. The LEA's proposed disciplinary actions against the two officers concerned and the remedial measure proposed were considered appropriate.</p> <p>(See paragraphs 6.74 to 6.76 of Chapter 6.)</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
	Surveillance	<p><u>Case 6.13</u></p> <p>A prescribed authorization was granted to an LEA in October 2019 for the conduct of Type 1 surveillance. It was assessed at the time of application that the surveillance operation sought to be authorized would unlikely obtain information subject to LPP. However, the panel judge imposed additional conditions to guard against the risk of obtaining LPP information when he approved the application.</p> <p>The LEA only reported the imposition of the additional conditions to the Commissioner in December 2019 but not in the relevant weekly report in October 2019.</p> <p>In December 2019, the LEA also reported to the Commissioner an incident that in one of the surveillance operations, a recording lasted about 30 seconds longer than it should. The Commissioner took the view that these 30 seconds might possibly be outside the ambit of the prescribed authorization such that this surveillance might be a non-compliance with the terms of the prescribed authorization.</p> <p>From the checking of the relevant weekly reports and the device register in respect of the prescribed authorization, the Commissioner observed that a surveillance device which was incompatible with the additional conditions had been issued on three occasions. During a periodical visit, the Commissioner required the LEA to provide explanations for the delay in reporting the imposition of the additional conditions and the issue of incompatible surveillance device. The LEA undertook to conduct an</p>

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			<p>investigation and inform the Commissioner of the outcome.</p> <p>The LEA submitted a full investigation report dated 31 March 2020 to the Commissioner under section 54 of the Ordinance. At the time of writing this report, a review on the case is still on-going. Details about the review will be reported in the next annual report.</p> <p>(See paragraphs 6.77 to 6.81 of Chapter 6.)</p>
		Interception (3 reviews)	<p><u>Other cases</u></p> <p>They were incidents of technical problems of the computer systems. Nothing untoward was found. The LEAs concerned had taken appropriate actions to remedy the problems.</p> <p>(See paragraph 6.82 of Chapter 6.)</p>
(h) Examination of protected products of past cases of non-compliance, irregularity or incident	4	Surveillance	<p><u>Past case (i)</u></p> <p>A report on a Type 2 surveillance operation conducted on an incoming call, allegedly from a person other than the subject of the executive authorization granted in 2010, was reported in Annual Report 2010.</p> <p>The then Commissioner had made a comment in Annual Report 2010 that the only means to ascertain whether there had been any non-compliance in the case was to listen to the recording of the incoming call. Given the express power to examine the protected products after the enactment of the Interception of Communications and Surveillance (Amendment) Ordinance 2016, the Commissioner had checked the preserved protected products of this case. The Commissioner found that</p>

Number of reviews conducted under section 41(1)	Interception/ Surveillance	Summary of reviews
		<p>the recording device had not captured any voice of the caller in the call and thus, the Commissioner concluded that there was no non-compliance involved in this case.</p> <p>(See paragraph 6.84 of Chapter 6.)</p>
	Interception & Surveillance (3 reviews)	<p><u>Other past cases</u></p> <p>The preserved protected products for three past cases, including two cases reported in 2009 and one in 2014, were examined in the report period. The Commissioner did not find anything that deviated from what had been reported to the relevant authority and/or the Commissioner.</p> <p>(See paragraph 6.83 of Chapter 6.)</p>

Section 41(2)

The Commissioner shall conduct reviews on cases in respect of which a report has been submitted to him under section 23(3)(b), 26(3)(b)(ii) or 54

Number of reviews conducted under section 41(2)		Interception/ Surveillance	Summary of reviews
(a) Report submitted under section 23(3)(b) by the head of department on cases in default of application being made for confirmation of emergency authorization within 48 hours of issue	Nil	Not applicable	For the report period, there was no report submitted under this category.
(b) Report submitted under section 26(3)(b)(ii) by the head of department on cases in default of application being made for confirmation of prescribed authorization or renewal issued or granted upon oral application within 48 hours of issue	Nil	Not applicable	For the report period, there was no report submitted under this category.
(c) Report submitted under section 54 by the head of department on any case of failure by the department or any of its officers to comply with any relevant requirement	2	Interception	<u>Outstanding case (i)</u> This case was first reported by an LEA in late 2014. The relevant court proceedings have not concluded at the time of writing this report. The reporting of this case can only be made when the relevant court proceedings have concluded. (See Outstanding case (i) at paragraph 6.6 of Chapter 6.)
		Surveillance	<u>Past case (ii)</u> The case concerned was a Type 1

Number of reviews conducted under section 41(2)	Interception/ Surveillance	Summary of reviews
		<p>surveillance with non-compliance reported in Annual Report 2010. The preserved protected products for this past case were examined in the report period.</p> <p>The case involved three surveillance operations. The non-compliance reported in Annual Report 2010 was on the third operation. After checking the protected products, I agreed with my predecessor that the third operation was a non-compliance as set out in Annual Report 2010. Notwithstanding this, clarifications were sought from the LEA concerned on the second operation. Upon conducting examination into the case, the LEA reported to the Commissioner that, pursuant to section 54 of the Ordinance, part of the second operation was conducted outside the ambit of the prescribed authorization concerned.</p> <p>The prescribed authorization was granted to the LEA for conducting Type 1 surveillance on meeting(s) between Subject 1 and Subject 2, with or without other person(s) in public place(s).</p> <p>The LEA deployed a senior officer to take charge of the Type 1 surveillance and two officers ('Officer A' and 'Officer B') to conduct the field operation. After arriving at the meeting place, Subjects 1 and 2 were seen meeting with other persons. Officer A then set up the device and started recording.</p> <p>About thirty minutes later, when Subjects 1 and 2 left the meeting place while the other persons still remained there, Officer A and Officer B continued the recording.</p> <p>After being notified by another team and confirmed that Subjects 1 and 2 were not anticipated to return to the meeting</p>

Number of reviews conducted under section 41(2)	Interception/ Surveillance	Summary of reviews
		<p>place, Officer A powered off the device. He immediately reported to the senior officer the conclusion of the operation but he did not mention the early departure of Subjects 1 and 2 and the continued recording after they had left the meeting place.</p> <p>In the evening of the same day, Officer A checked the recording and realised that the recording did not capture Subjects 1 or 2 or any of the persons attending the meeting. He immediately reported the outcome of the recording to the senior officer. The time when Subjects 1 and 2 left the meeting place and the cessation time of recording were documented.</p> <p>An officer-in-charge of the investigation ('Officer C') received the relevant documents and the recording from Officer A. She understood from Officer A that the operation had not been successful and the recording contained nothing of evidential value. She was not aware that the recording had continued for ten minutes after the Subjects had left the meeting place.</p> <p>In conducting a review of the operation, nothing special was raised by the senior officer when the documents were submitted to a reviewing officer ('RO').</p> <p>The LEA was of the view that the unauthorized surveillance was attributed to the lack of vigilance and inadequacy in performance in the execution of the operation by Officer A. However, there was no indication of any sinister motive on his part to conceal the absence of subjects from the meeting as he had recorded the fact in relevant document.</p> <p>The LEA recommended that a verbal warning (disciplinary) be given to Officer A given the fact that he did not</p>

Number of reviews conducted under section 41(2)		Interception/ Surveillance	Summary of reviews
			<p>stop the recording upon the subjects leaving the meeting place.</p> <p>The LEA also proposed that a verbal warning (disciplinary) be given to the senior officer and an advice (non-disciplinary) be given to Officer C. For Officer B and RO, they had left the LEA and their accounts of the incident could not be obtained.</p> <p>As time passed, clear guidelines and more training had been provided to frontline officers who were responsible for carrying out ICSO duties. Besides, frontline officers involved in surveillance operations were required to record details of what they had reported to the supervisor in respect of the operations within a specified time frame. Such record would also be submitted together with other necessary documents to the reviewing officers for review.</p> <p>After reviewing the case, the Commissioner considered that this was a case of non-compliance. The continuation of surveillance operation on a meeting without the presence of Subjects 1 and 2 did not comply with the terms of the prescribed authorization. However, the Commissioner found no evidence showing that there was foul play, ulterior motive or deliberate act involved in the unauthorized surveillance. The Commissioner agreed with the LEA's findings. The recommended actions against the officers involved as well as the improvement measures were considered appropriate.</p> <p>(See paragraphs 6.85 to 6.98 of Chapter 6.)</p>

Table 6

Number and broad nature of cases of irregularities or errors identified in the reviews [section 49(2)(d)(ii)]

Section 41(1)

Number of cases of irregularities or errors identified in the reviews under section 41(1)		Interception/ Surveillance	Broad nature of irregularities or errors identified
(a) Reviews of LPP cases	9	Interception	<u>Case 6.1</u> An officer listened to a call which involved a prohibited telephone number, amounting to a breach of the additional conditions imposed by the panel judge on the prescribed authorization concerned.
		Interception	<u>Case 6.3</u> A supervisor failed to timely report an alias of the subject to the panel judge as required under section 58A of the Ordinance and paragraph 116 of the COP.
		Interception	<u>Case 6.4</u> Delay in reporting the arrest status of the subject to the panel judge.
		Interception	<u>Case 6.5</u> Telecommunications interception of three facilities (including one facility from each of the two LPP cases) was inadvertently interrupted.
		Interception	<u>Case 6.6</u> An officer accessed interception products during suspension of monitoring of interception.

Number of cases of irregularities or errors identified in the reviews under section 41(1)		Interception/ Surveillance	Broad nature of irregularities or errors identified
		Interception	<u>Case 6.9</u> An officer failed to report to his supervisor a call which might indicate heightened LPP likelihood.
		Interception	<u>Case 6.10</u> An earlier call with heightened LPP likelihood was not reported to the panel judge.
		Interception	<u>Case 6.11</u> An earlier call with heightened LPP likelihood was not reported to the panel judge.
		Interception	<u>Case 6.12</u> Failure in documenting properly the result of an assessment on the likelihood of obtaining LPP information arising from an intercepted call. (For details, see item (g) under section 41(1) in Table 5 and Chapter 6.)
(b) Examination of protected products of past cases of non-compliance, irregularity or incident	1	Surveillance	<u>Past case (i)</u> Type 2 surveillance was conducted on an incoming call which was allegedly made from a person other than the subject of the executive authorization. (For details, see item (h) under section 41(1) in Table 5 and Chapter 6.)

Number of cases of irregularities or errors identified in the reviews under section 41(1)		Interception/ Surveillance	Broad nature of irregularities or errors identified
(c) Other reviews	8	Surveillance	<u>Outstanding case (ii)</u> Surveillance was conducted when the subject was not present in the specified premises, which did not comply with the terms of the prescribed authorization.
		Interception	<u>Case 6.2</u> The user identity of the officer as stated in the ATRs in respect of monitoring of interception was incorrect.
		Interception	<u>Case 6.7</u> Inaccurate information provided in an REP-11 report submitted to the panel judge.
		Surveillance	<u>Case 6.8</u> Discrepancy in the recorded time of two covert surveillance products of the same operation.
		Surveillance	<u>Case 6.13</u> Delay in reporting to the Commissioner the imposition of additional conditions on a prescribed authorization, issue of surveillance device which was incompatible with the additional conditions and surveillance might have been conducted not in compliance with the terms of the prescribed authorization.
		Interception	<u>Three other cases</u> These are cases involving technical problems of the computer systems.
			(For details, see item (g) under section 41(1) in Table 5 and Chapter 6.)

Section 41(2)

Number of cases of irregularities or errors identified in the reviews under section 41(2)		Interception/ Surveillance	Broad nature of irregularities or errors identified
(a) Reviews on cases in default of application being made for confirmation of emergency authorization within 48 hours as reported by the head of department under section 23(3)(b)	Nil	Not applicable	As mentioned in Table 5 above, there was no report submitted under this category.
(b) Reviews on cases in default of application being made for confirmation of prescribed authorization or renewal issued or granted upon oral application within 48 hours as reported by the head of department under section 26(3)(b)(ii)	Nil	Not applicable	As mentioned in Table 5 above, there was no report submitted under this category.
(c) Reviews on non-compliance cases as reported by the head of department under section 54	1 ^{Note 6}	Interception	<u>Outstanding case (i)</u> This case was brought forward from the previous annual report under this category and it is inappropriate to report on the review of the case in this report due to ongoing court proceedings.
		Surveillance	<u>Past case (ii)</u> Type 1 surveillance was conducted outside the ambit of the prescribed authorization.

Note 6 The number of reviews does not include the 'Outstanding case (i)'

Number of cases of irregularities or errors identified in the reviews under section 41(2)	Interception/ Surveillance	Broad nature of irregularities or errors identified
		(For details, see item (c) under section 41(2) in Table 5 and Chapter 6.)

Table 7

Number of applications for examination that have been received by the Commissioner [section 49(2)(d)(iii)]

Number of applications received	Applications for examination in respect of			
	Interception	Surveillance	Both Interception and Surveillance	Cases that could not be processed
17	4	0	6	7

Table 8

Respective numbers of notices given by the Commissioner under section 44(2) and section 44(5) further to examinations [section 49(2)(d)(iv)]

Number of notices to applicants given by the Commissioner		Nature of applications for examination		
		Interception	Surveillance	Both Interception and Surveillance
Number of cases that the Commissioner had found in the applicant's favour [section 44(2)]	0	—	—	—
Number of cases that the Commissioner had not found in the applicant's favour [section 44(5)] ^{Note 7}	10	4	0	6

^{Note 7} Of the ten notices, five were issued during the report period and five thereafter.

Table 9

**Number of cases in which a notice has been given by
the Commissioner under section 48 [section 49(2)(d)(v)]**

	Number of cases in which a notice has been given in relation to	
	Interception	Surveillance
Notice to the relevant person by the Commissioner stating that he considers that there has been a case of interception or surveillance carried out by an officer of a department without the authority of a prescribed authorization and informing the relevant person of his right to apply for an examination [section 48(1)]	0	0

Table 10

**Broad nature of recommendations made by the Commissioner
under sections 50, 51 and 52 [section 49(2)(d)(vi)]**

Recommendations made by the Commissioner		Interception/ Surveillance	Broad nature of recommendations
Reports to the Chief Executive on any matter relating to the performance of the Commissioner's functions [section 50]	Nil	Not applicable	Not applicable
Recommendations to the Secretary for Security on the COP [section 51]	Nil	Not applicable	Not applicable
Recommendations to departments for better carrying out the objects of the Ordinance or the provisions of the COP [section 52]	4	Interception & Surveillance	<p>(a) Providing justifications for not restricting monitoring of interception to officers at a specific rank or above in LPP and JM cases.</p> <p>(b) Reporting to the Commissioner cases not involving LPP information or JM but additional conditions are imposed on the prescribed authorizations by the panel judge and preserving the related protected products for examination by the Commissioner.</p> <p>(c) Making record of assessment on heightened LPP likelihood arising from an intercepted communication.</p> <p>(d) Reporting contents of the communication from which the arrest of the subject is</p>

Recommendations made by the Commissioner		Interception/ Surveillance	Broad nature of recommendations
			<p>revealed in the section 58 report.</p> <p>(See paragraph 7.2 of Chapter 7.)</p>

Table 11

Number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or surveillance carried out pursuant to a prescribed authorization [section 49(2)(d)(vii)]

	Number of cases
Interception	0
Surveillance	1

Table 12

Number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 42, 47, 52 or 54 and the broad nature of such action [section 49(2)(d)(viii)]

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<u>Case 1</u> Interception	An officer failed to remove access right to interception products in respect of an interception operation completely as required. (See paragraphs 6.24 to 6.28 of Chapter 6 of Annual Report 2018.)	Verbal advice
<u>Case 2</u> Interception	An officer failed to report to her supervisor a call indicating heightened LPP likelihood. (See paragraphs 6.43 to 6.47 of Chapter 6 of Annual Report 2018.)	Verbal advice
<u>Case 3</u> Interception	An officer accessed an interception product during the period when monitoring of the interception operation should have been put on hold. (See paragraphs 6.64 to 6.67 of Chapter 6 of Annual Report 2018.)	Verbal advice
<u>Case 4</u> Interception	An officer failed to make record of a call with possible heightened LPP likelihood which was thus not reported to the panel judge. (See paragraphs 6.114 to 6.120 of Chapter 6 of Annual Report 2018.)	Verbal advice

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<p><u>Case 5</u> Interception</p>	<p>(i) An officer wrongly assigned access right to interception products to an officer below the rank specified in an additional condition of the related prescribed authorization, leading to non-compliance of the additional condition that monitoring of the interception operation authorized under the prescribed authorization should be undertaken by officers not below the rank specified therein.</p> <p>(ii) A senior officer, who approved the removal of the wrongly assigned access right, failed to discover the non-compliance mentioned in (i) above.</p> <p>(iii) A senior officer, who sought approval from the senior officer mentioned in (ii) above for the removal of the wrongly assigned access right, failed to discover the non-compliance mentioned in (i) above.</p> <p>(See paragraphs 6.91 to 6.100 of Chapter 6 of Annual Report 2018.)</p>	<p>Verbal warning</p> <p>Verbal warning</p> <p>Verbal warning</p>
<p><u>Case 6</u> Surveillance</p>	<p>An officer-in-charge made mistakes in the ICSO applications documents repeatedly within a short period of time.</p> <p>(See paragraphs 6.74 to 6.84 of Chapter 6 of Annual Report 2018.)</p>	<p>Verbal warning</p>
<p><u>Case 7</u> Interception</p>	<p>An officer failed to report information accurately in an REP-11 report to the panel judge.</p> <p>(See paragraphs 6.107 to 6.109 of Chapter 6 of Annual Report 2018.)</p>	<p>Verbal advice</p>

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<p><u>Case 8</u> Interception</p>	<p>(i) An officer failed to check the arrest status of the subject correctly, leading to delay in reporting to the panel judge the previous arrest of the subject.</p> <p>(ii) The supervisor of the officer mentioned in (i) above failed to counter-check the checking result reported by the officer.</p> <p>(iii) The supervisor of the officer mentioned in (ii) above had supervisory accountability for the incident.</p> <p>(See paragraphs 6.34 to 6.38 of Chapter 6.)</p>	<p>Verbal warning</p> <p>Verbal warning</p> <p>Verbal advice</p>
<p><u>Case 9</u> Interception</p>	<p>An officer failed to report to the panel judge an alias of the subject which surfaced during interception as soon as reasonable practicable as required by the Ordinance and the COP.</p> <p>(See paragraphs 6.29 to 6.33 of Chapter 6.)</p>	<p>Verbal advice</p>
<p><u>Case 10</u> Surveillance</p>	<p>(i) The officer did not stop the recording upon the subjects leaving the meeting place, resulting in an excessive recording of about ten minutes which was outside the ambit of the prescribed authorization.</p> <p>(ii) The senior officer, as the officer-in-charge of the Type 1 surveillance, was not alert that the operation might have been conducted outside the ambit of the prescribed authorization.</p> <p>(See paragraphs 7.162 to 7.225 of Chapter 7 of Annual Report 2010 and paragraphs 6.85 to 6.98 of Chapter 6.)</p>	<p>Verbal warning</p> <p>Verbal warning</p>

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<p><u>Case 11</u> Surveillance</p>	<p>An officer-in-charge of the operation failed to interpret the terms of the prescribed authorization, resulting in carrying out covert surveillance outside the ambit of the prescribed authorization.</p> <p>(See paragraph 6.106 of Chapter 6 of Annual Report 2018 and paragraphs 6.7 to 6.18 of Chapter 6.)</p>	<p>Verbal warning</p>
<p><u>Case 12</u> Interception</p>	<p>An officer failed to report to his supervisor a call which might indicate heightened LPP likelihood.</p> <p>(See paragraphs 6.60 to 6.63 of Chapter 6.)</p>	<p>Verbal advice</p>

8.2 In accordance with section 49(2)(e) of the Ordinance, the Commissioner is required to give an assessment on the overall compliance with the relevant requirements during the report period. Such assessment and the reasons in support can be found in Chapter 9.

CHAPTER 9

REVIEW OF COMPLIANCE BY LAW ENFORCEMENT AGENCIES

Overall compliance

9.1 As set out in section 40 of the Ordinance, the functions of the Commissioner are to oversee the compliance by the LEAs and their officers with the relevant requirements and to conduct reviews, etc. It is stipulated under section 49(2)(e) of the Ordinance that the Commissioner shall set out in the annual report an assessment on the overall compliance with the relevant requirements during the report period. My assessment of the overall performance of the LEAs and their officers in their compliance with the relevant requirements of the ICSO in 2019 is set out below.

Preparation of applications

9.2 The first and foremost of the requirements under the Ordinance is that any statutory activity can only be lawfully and properly conducted by an officer of an LEA pursuant to a prescribed authorization granted by a relevant authority. Whether a prescribed authorization should be granted is expressly based on the necessity and proportionality principles i.e. the interception or covert surveillance is necessary for, and proportionate to, the purpose sought to be furthered by carrying it out upon balancing the relevant factors against the intrusiveness of the interception or covert surveillance on any person who is to be the subject of or may be affected by the interception or covert surveillance; and considering whether the purpose sought to be furthered by carrying out

the interception or covert surveillance can reasonably be furthered by other less intrusive means.

9.3 During the report period, only four of the 1,314 applications for interception were refused and the reason for refusal was insufficient materials to support the allegations put forth. As regards covert surveillance, all the 25 applications were granted by the relevant authorities.

9.4 In general, the LEAs were observed to have continued to adopt a cautious approach in preparing their applications for interception and covert surveillance operations.

Reviews by the Commissioner

9.5 There were different ways to review the LEAs' compliance with the requirements of the Ordinance in respect of interception and covert surveillance as set out in paragraph 2.17 of Chapter 2 and paragraph 3.19 of Chapter 3. These included checking of the weekly reports submitted by the LEAs and the PJO, and examination of the contents of the LEA files and documents as well as the protected products during visits to the LEAs. Where necessary, the LEA concerned would be requested to respond to queries. For interception operations, counter-checking the facilities intercepted with non-LEA parties such as CSPs and through other means would be done. For covert surveillance operations, the records kept by the surveillance device recording system of the LEAs would be checked.

9.6 In the report period, the interception/covert surveillance operations were in general conducted pursuant to prescribed authorizations granted by the relevant authorities and the additional conditions imposed but there were still a few cases of non-compliance as

reported in Chapter 6. There was no sign of abuse of surveillance devices for any unauthorized purposes.

Handling of LPP and JM cases

9.7 The COP obliges the concerned LEA to notify the Commissioner of cases that are likely to involve LPP information or JM. The Commissioner is also timeously alerted to cases involving or possibly involving LPP information or JM through the examination of the weekly reports submitted by the LEAs, with sanitised copies of the relevant REP-11/REP-13 reports reporting on any material change in circumstances after the issue of a prescribed authorization including changed LPP and JM risks.

9.8 Through the examination of protected products, I am able to check the veracity of the gist of the communications or information stated in the REP-11/REP-13 reports and whether there were any communications or information subject to LPP or with JM that had been accessed by the LEA officers but not reported to the relevant authority.

9.9 A total of 175 new LPP and JM cases were reported in 2019. Except 15 LPP cases which were still on-going beyond the report period, review of 155 LPP and five JM cases had been completed. Of the 155 LPP cases, except for those specifically mentioned in Cases 6.4, 6.5, 6.6, 6.9, 6.10, 6.11 and 6.12 and one case involving technical problem of the computer systems mentioned in paragraph 6.82 of Chapter 6, nothing untoward was found for these cases. As for the five JM cases, they were all found in order. There was one case on actual obtainment of information subject to LPP as detailed in paragraphs 4.14 to 4.17 of Chapter 4. At the time of application, it had already been assessed that the operation sought to be authorized would likely obtain information subject to LPP and so the panel judge had imposed additional conditions that all the surveillance products should be passed to a dedicated unit to screen out, if any, information

subject to LPP. I have checked and confirmed that the LEA had complied with the additional conditions and the surveillance products passed on to the investigators did not contain any LPP information.

9.10 With regard to the 29 on-going LPP cases reported in Annual Report 2018, the authorized operations concerned were discontinued in 2019. Except for the case referred to in Case 6.3 of Chapter 6 and the case involving technical problem of the computer system mentioned in paragraph 6.130 of the Annual Report 2018, nothing untoward was found.

9.11 While the LEAs were observed to have recognised the importance of protecting information which might be subject to LPP or JM and have continued to adopt a very cautious approach in handling these cases, there were still several cases reflecting the failure of some officers in exercising enough vigilance and care on certain occasions as revealed in the cases reported in Chapter 6. The LEAs concerned had continued to remind their officers to be vigilant when they encounter situations indicating heightened LPP likelihood in the course of performing interception monitoring duties. For an officer who persistently failed to perform interception monitoring duties vigilantly in guarding against the risk of obtaining information subject to LPP as mentioned in Case 6.11 of Chapter 6, the LEA concerned had removed the officer from carrying out such duties.

9.12 During the report period, the protected products of six LPP cases reported before 2016 were also examined. The examination of the protected products of these six cases did not reveal anything to justify deviation from the assessments given by my predecessors or myself on the handling of LPP cases reported in the past years.

Non-compliance, irregularities or incidents

9.13 Under section 54 of the Ordinance, the head of an LEA is required to submit a report to the Commissioner if he considers that there may have been any case of failure to comply with any relevant requirement of the Ordinance, irrespective of whether the failure is due to the fault of the LEA or its officers or not. LEAs are also required to report to the Commissioner cases of irregularity or even simply incidents. Hence, all cases of possible non-compliance are brought to the attention of the Commissioner for examination and review without any delay. Furthermore, whenever necessary, the LEAs are required to provide a report, clarification or explanation for anything unusual detected in the course of examination of documents and protected products by the Commissioner. In 2019, there were 16 cases of non-compliance/irregularity/incident.

9.14 For all the completed cases reported in Chapter 6, I did not find any deliberate disregard of the statutory provisions or the COP nor have I found any ulterior motive or ill will on the part of the officers involved. However, I considered that the non-compliance case on Type 1 surveillance involving misinterpretation of a term of the prescribed authorization concerned as detailed in paragraphs 6.7 to 6.18 of Chapter 6 was rather alarming. It reflected the lack of understanding and professional knowledge of the officer concerned in discharging ICSO duties. Such kind of mistakes made by an officer of a rather senior level responsible for ICSO duties and the mistakes were left unnoticed after a series of internal reviewing process of the LEA is a great concern to me. Coupled with the track record of the officer concerned involving in several other irregularities on ICSO duties in recent years, I casted doubt on the reliability of the officer in discharging ICSO duties. I appreciated that the LEA had taken my advice to reconsider the suitability of the officer in undertaking ICSO duties and posted out the officer subsequently.

9.15 Most of the cases mentioned under Cases 6.1 to 6.12 were consequences of inadvertence or carelessness of the officers concerned, reflecting that some of the officers were still not vigilant and cautious enough in discharging ICSO duties. I consider it of utmost importance that all LEAs and their officers should make every effort to ensure that similar mistakes would not be made again. The heads of LEAs should endeavour to provide their officers with sufficient advice and training to facilitate them to better perform the ICSO duties especially when officers are newly deployed to take up ICSO duties either on a long term basis or in short term acting capacity. Furthermore, officers of the LEAs should stay alert and exercise care in different stages of the operations conducted under the ICSO.

Response from LEAs

9.16 I am pleased to see that in the report period, LEAs continued to be positive to my recommendations in every aspect aiming for better operation of the ICSO regime and took initiative to implement system enhancements to prevent recurrence of technical mistakes or to avoid human errors.

CHAPTER 10

ACKNOWLEDGEMENT AND WAY FORWARD

Acknowledgement

10.1 During the report period, various parties including the panel judges, the Security Bureau, the LEAs and the CSPs continued to render great assistance to me in performing the oversight and reviewing functions under the ICSO. I would like to take this opportunity to express my heartfelt gratitude to each one of them. My tasks as the Commissioner could not be carried out so smoothly and efficiently without their unstinting assistance and cooperation.

Way forward

10.2 The ICSO aims to strike a balance between the need for the prevention and detection of serious crime 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. The legislative amendments in 2016 enabling me to have the express power of examining the protected products have taken effect for over three years. The working arrangements on the examination of protected products have been well established which exerted effective deterrence against any deliberate non-compliance of the LEAs with the Ordinance. For the better operation of the ICSO regime, a number of suggestions and recommendations have been made on the procedural matters and control mechanism to remedy any deficiencies or irregularities over the years. Whenever irregularities or incidents occurred involving new situations or problems, I would recommend targeted measures for reducing, if not eliminating, similar irregularities and non-compliance in future. The recommendations have

been well accepted and implemented by the LEAs to enhance compliance with the Ordinance and the COP. Nevertheless, irregularities and mistakes were still found. It was mainly due to the lax attitude and inadvertence of individual officers and occasionally due to the lack of sufficient knowledge on ICSO-related duties of inexperienced officers rather than deficiencies in the control systems. Most of the irregularities in fact could be avoided if the officers concerned were more cautious and attentive to their work. Provision of training and guidance as well as enhancements in the procedures and technologies could help minimising the risk of human errors. However, a serious attitude in discharging the ICSO duties and in observing all the procedures and guidelines is equally, if not more, important in achieving full compliance with the ICSO requirements.

10.3 I look forward to the concerted efforts of each and every one of the officers involved in ICSO duties in observing the spirit and requirements of the Ordinance and also the continuous support and cooperation of all the parties involved in facilitating the oversight work of the Commissioner.