Annual Report 2012 to the Chief Executive

by

The Commissioner on
Interception of Communications
and Surveillance

June 2013

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.3 電話 Tel. No.:

來函檔號 Your. ref. 傳真 Fax No.:

27 June 2013

The Honourable C Y Leung, GBM, GBS, JP
The Chief Executive
Hong Kong Special Administrative Region
People's Republic of China
Tamar
Hong Kong

CONFIDENTIAL

Dear Sir,

Annual Report for the Year 2012

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 2012, together with its Chinese translation.

Yours sincerely,

(D. G. Saw)
Commissioner on Interception of
Communications and Surveillance

Encl: Annual Report for 2012

香港灣仔皇后大道東 248 號 15 樓 1501-1504 室
Units 1501-1504, 15/F, 248 Queen's Road East, Wanchai, Hong Kong

CONTENTS

Tables in Chapter 9 ***Page***

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	Interception of Communications and Surveillance Ordinance
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non-ICSO device register	register of devices withdrawn based on loan requests for surveillance devices for purposes in respect of which no prescribed authorization is required and of such devices returned
non-ICSO purpose	purpose which is not related to ICSO
Ordinance	Interception of Communications and Surveillance Ordinance
panel judge	the panel judge appointed under section 6 of the Ordinance
PJO	Panel Judges' Office
prohibited number	specified telephone number the calls through which are prohibited from being listened to
renewal application	application for renewal of a prescribed authorization
REP-11 report	report on material change of circumstances or initial material inaccuracies under a prescribed authorization made on form REP-11

Reported LPP Call	a call which might involve LPP information or likely 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 described in the Ordinance
the report period	the period from 1 January to 31 December 2012
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 panel judges to provide information to the Commissioner once every week

CHAPTER 1

INTRODUCTION

Introduction

1.1 Over six years have elapsed since the coming into operation of the Interception of Communications and Surveillance Ordinance, Cap 589 ('Ordinance' or 'ICSO') and the establishment of the office of the Commissioner on Interception of Communications and Surveillance ('Commissioner'). I was appointed as Commissioner on 17 August 2012 for a term of three years and am required pursuant to section 49 of the Ordinance to report to the Chief Executive for the 12-month period ending on 31 December in each year. This is my first report. The period of this report overlaps with the term of office of my predecessor, Mr. Woo Kwok-hing, GBS, who was the first Commissioner appointed and served two terms, the second of which expired on 16 August 2012.

1.2 At the outset of this report, I would like to acknowledge the extraordinary contribution made by my predecessor and the staff in the establishment and operation of the Secretariat, Commissioner on Interception of Communications and Surveillance ('Secretariat').

1.3 Notwithstanding the limited time I have been the Commissioner, it is apparent to me that much has been achieved in the relatively short time since the Ordinance came into effect and the office of the Commissioner was established. It is equally apparent that this is directly attributable to the dedication, focus and diligence of my predecessor. Upon assuming this office, I took charge of a

sophisticated and efficient Secretariat which had been established, developed, and refined under the direction of Mr. Woo. Mr. Woo's energy and dedication to his responsibilities in his two terms as Commissioner are manifest by this. I sincerely trust that I will, as Commissioner, discharge the oversight and review functions of the Commissioner fully and effectively as did my predecessor.

1.4 Shortly after I took office, I met with the heads of the four law enforcement agencies ('LEAs'), namely, the Commissioner of Customs and Excise, the Commissioner of Police, the Director of Immigration and the Commissioner, Independent Commission Against Corruption, and was briefed by them and their senior officers as to the operation of the ICSO in respect of each of those agencies. In each case, I was assured of their support, ongoing co-operation, and in the case of each of their respective agencies, a determination to ensure that the objectives of the ICSO should be sustained. I was also assured that there would be strict compliance with the Ordinance and the Code of Practice ('COP') issued under section 63 of the Ordinance.

1.5 In November 2012, I met with senior officers of the Security Bureau to discuss the progress of recommendations made in the Annual Report 2011. I am pleased to advise that much progress has been made.

Interception of Communications and Surveillance Ordinance

1.6 The scheme of the ICSO is to envelop the activities of the four LEAs in the interception of communications, through the post or through the use of telecommunications facilities, and in covert surveillance by the use of surveillance devices (collectively called 'statutory activities') in a statutory framework, so as to ensure that

these activities cannot be lawfully and properly carried out unless the relevant requirements stipulated in the Ordinance are satisfied.

1.7 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 COP issued by the Secretary for Security.

1.8 Whether a prescribed authorization should be granted is expressly based on the necessity and proportionality principles, and 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 crimes 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.

1.9 The task of the Commissioner is to supervise and review the actions of the LEAs and their officers regarding their compliance with all such requirements as described above. These objects and spirit of the Ordinance must constantly be borne in mind when these functions are carried out.

1.10 In his two terms as Commissioner, my predecessor together with the staff of the Secretariat have designed various ways and means to perform and facilitate the operation of the Ordinance.

These have been either put forward to and implemented by the LEAs as requirements or procedures adopted pursuant to section 53 of the Ordinance, or they have been presented to the LEAs and the Security Bureau as advices, suggestions or recommendations, where appropriate.

Continuous improvements

1.11 Despite the diligence of the responsible LEA officers and their supervisors, problems and difficulties from time to time persist in the implementation of procedures in place to ensure compliance with the Ordinance and COP. I have observed that most of the irregularities encountered and mistakes made by LEA officers were attributable to their inadvertence or negligence, which were uniquely related to the individuals concerned, rather than defects in any of the control systems. There is, however, ongoing consultation with the LEAs to ensure that these are addressed and where necessary changes are made to procedures.

1.12 Part of the function of the Commissioner is to be involved in advising the LEAs in designing ways to resolve hitherto unexpected problems and taking the opportunity to anticipate others. This engagement is ongoing and operates in the best interest of all the LEAs and also for the benefit of the society in which we live because improvements can be continuously made to tackle existing and anticipated situations with the aim to cause the least invasion to the privacy and other rights of individuals. I will be working together with the LEAs to further reduce the incidence of irregularities, inaccuracies and mistakes, an objective addressed by my predecessor on more than one occasion.

1.13 The majority of my predecessor's most recent recommendations and suggestions on various procedural matters have been accepted by the Security Bureau and the LEAs, or they have made practical arrangements to remedy the adverse effect of the defects or deficiencies intended to be addressed by such recommendations and suggestions. This remains an ongoing process under my term as Commissioner.

Transparency

1.14 This report follows the format established by my predecessor and like him I consider it necessary to continue the practice of providing the utmost transparency of the work of the Commissioner in this annual report, save to take great care not to divulge any information the disclosure of which may prejudice the prevention or detection of crime or the protection of public security, as expressly required by various provisions of the Ordinance. With that in mind, I hope I have included as much information as possible insofar as its publication does not amount to contravention of this non-prejudice principle.

[This page is left blank.]

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 1,168 written applications for interception made by the LEAs, of which 1,161 were granted and seven were refused by the panel judges. Among the successful applications, 506 were for authorizations for the first time ('fresh applications') and 655 were for renewals of authorizations that had been granted earlier ('renewal applications').

Reasons for refusal

2.3 Of the seven refused applications, one was a fresh application and six were renewal applications. The refusals were mainly due to the following reasons:

(a) no or limited useful information had been obtained from the interception operation conducted under previous authorizations; or

(b) inadequate/insufficient materials to support the allegations put forth.

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, 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. Paragraph 92 of 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 83% 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 43 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 9 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, should cause an

interception (and also covert surveillance) to be discontinued if he is of the opinion that a ground for discontinuance 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.

2.11 The number of authorizations for interception revoked 'fully' under section 57 during the report period was 419. Another 62 cases involved the cessation of interception in respect of some, but not all, of the telecommunications facilities approved under a prescribed authorization, so that while the prescribed authorization is 'partially' revoked, interception of the remaining approved facilities continued to be in force.

2.12 The grounds for discontinuance were mainly that the interception operation was not or no longer productive, the subject had stopped using the telecommunications facility concerned for his criminal activities, or the subject was arrested.

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 information which may be subject to legal professional privilege ('LPP') 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 79 arrests but only one section 58 report was made to the panel judge. For this section 58 report, as the relevant prosecution against the subject in question had already been concluded at the time of receipt of the report, the panel judge allowed the LEA to continue with the interception. As regards the other arrest cases, decisions were made by an officer of the LEAs concerned to discontinue the interception operation 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.

Authorizations with five or more previous renewals

2.14 There were 41 authorizations for interception with five or more previous renewals within the report period. As these cases had lasted for quite a long period of time, particular attention was paid to see whether the renewals were granted properly and whether useful information had been obtained through the interception operations. All the cases with six renewals and some of their further renewals were checked and found in order during inspection visits to the LEAs.

Effectiveness of interception

2.15 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 crimes and the protection of public

security. Information gathered from interception can very often lead to a fruitful and successful conclusion of an investigation. During the report period, a total of 70 persons, who were subjects of prescribed authorizations, were arrested as a result of or further to interception operations. In addition, 164 non-subjects were also arrested consequent upon the interception operations.

Procedure of oversight for interception

2.16 There were three different ways by which compliance with the requirements of the Ordinance in respect of interception by the LEAs was reviewed:

(a) checking of the weekly reports submitted by the LEAs and the Panel Judges' Office ('PJO');

(b) periodical examination of the contents of the LEA files and documents during inspection visits to the LEAs; and

(c) 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

2.17 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.

2.18 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 journalistic material from the proposed operation, etc. Sensitive information such as the case details, progress of the investigation, identity and particulars of the subject and others, etc is not required and therefore obliterated or sanitized, so that such information will always be kept confidential with minimal risk of leakage.

2.19 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, clarifications and explanations were sought from the LEAs and/or the PJO as and when necessary.

Checking of cases during inspection visits

2.20 Should the Commissioner perceive a need, clarification and explanation on the weekly report forms would also be sought in the

inspection 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 original of the applications, reports on discontinuance, reports on material change of circumstances, reports on initial material inaccuracies, case files and internal review documents, etc. Such inspection 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.

2.21 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.

2.22 In addition to matters relating to minor discrepancies in the weekly reports from the LEAs and the PJO, a total of 617 applications for interception, including granted authorizations and refused applications, and 223 related documents/matters had been checked during the Commissioner's inspection visits to the LEAs in the report period.

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

2.23 Apart from examining the weekly returns from the LEAs against those from the PJO, and conducting periodical checks of the relevant files and documents at the LEAs' offices, other measures have also been made available to and adopted by the Secretariat for further checking the interceptions conducted by the LEAs.

2.24 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

2.25 In 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 department 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 this report period, there were a total of

(a) six written applications for Type 1 surveillance, all were fresh applications; and

(b) 11 written applications for Type 2 surveillance including nine fresh and two renewal applications.

No application for Type 1 or Type 2 surveillance was refused.

Emergency authorizations

3.4 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 by reason of an imminent risk of death or serious bodily harm, 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.

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

Oral applications

3.6 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 to refuse the application.

3.7 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.

3.8 During this report period, there were two oral applications for Type 2 surveillance, both of which were granted. No oral application for Type 1 surveillance was made by the LEAs.

Duration of authorizations

3.9 The maximum duration authorized for both Type 1 and Type 2 surveillance allowed under the Ordinance is three months. The longest approved duration of Type 1 surveillance granted in this report period was about four days whereas the shortest one was less than a day. Overall, the average duration for such authorizations was about two days. In this report period, the longest approved duration of Type 2 surveillance granted was about 16 days while the shortest one was less than a day. The overall average duration of Type 2 surveillance executive authorizations was about six days.

Authorizations with five or more previous renewals

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

Offences

3.11 The major categories of offences for the investigation of which prescribed authorizations were issued or renewed for surveillance (both Type 1 and Type 2) during the report period are set out in Table 2(b) in Chapter 9.

Revocation of authorizations

3.12 During the report period, six Type 1 surveillance operations were discontinued under section 57 before the natural expiration of the prescribed authorizations. The grounds for discontinuance were mainly that the surveillance had been carried out, the anticipated event to be monitored did not materialize or the subject was arrested. 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 six discontinuance cases, two prescribed authorizations concerned were subsequently revoked by the panel judge. For the remaining four cases, the 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 authorization.

3.13 As regards Type 2 surveillance cases, during this report period, ten Type 2 surveillance operations were discontinued under section 57 before their natural expiration. The grounds for discontinuance were mainly that the subject was arrested, the surveillance had been carried out or the operation was not productive. Nine of the prescribed authorizations concerned were subsequently revoked by the authorizing officer. For the remaining one, the prescribed authorization concerned had expired by the time the authorizing officer received the discontinuance report. Hence, he could only note the discontinuance instead of revoking the prescribed authorization.

3.14 Revocation of authorizations is expressly provided for in section 58 of the Ordinance for covert surveillance when the subject(s) of the covert surveillance has been arrested. During this report period, no report was made to the relevant authority under section 58 seeking continuation of prescribed authorizations in spite of the arrest of the subject. Instead, those prescribed authorizations 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 they were appreciative of the risk of obtaining LPP information after an arrest.

Application for device retrieval warrant

3.16 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 upon the completion of the surveillance operation, successful or otherwise.

Effectiveness of covert surveillance

3.17 As a result of or further to surveillance operations, be it Type 1 or Type 2, a total of 12 persons who were subjects of the prescribed authorizations were arrested. In addition, 13 non-subjects were also arrested in consequence of such operations.

Procedure of oversight

3.18 The compliance with the requirements of the Ordinance in respect of covert surveillance by the LEAs was reviewed in three different ways:

(a) checking of the weekly reports submitted by the LEAs and the PJO;

(b) periodical examination of the contents of the LEA files and documents during inspection visits to the LEAs; and

(c) 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

3.19 Weekly reports submitted by the LEAs and 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 surveillance.

Checking of cases during inspection visits

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

3.21 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 inspection visits to the LEAs in this report period, apart from the clarification of matters relating to minor discrepancies in the weekly reports, a total of seven applications for Type 2 surveillance and seven related documents/matters had been checked. Generally speaking, while there were some areas for improvement, the cases were found to be in order.

3.22 During the inspection visits to the LEAs in this report period, seven applications for Type 1 surveillance and nine related documents/matters had been checked.

3.23 In examining the weekly reports, it was noted that there were some cases where surveillance devices were withdrawn under a prescribed authorization but no surveillance operation was carried out. The Commissioner considered the following matters required further enquiry:

(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.

All such cases were included for examination in the inspection visits, at which the Commissioner checked the relevant case documents and requested the LEA concerned to answer queries. The explanations given by the LEA for all these cases were satisfactory and there was no sign of use of surveillance devices for any unauthorized purposes.

Checking of surveillance devices

3.24 Having regard to the fact that covert surveillance, be it Type 1 or Type 2 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 device register of devices withdrawn based on loan requests with a prescribed authorization in support and a separate device 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.

3.25 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 list and device registers are submitted to the Commissioner on a regular basis. 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 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

3.26 Apart from the checking of inventory lists and device registers of surveillance devices managed by the LEAs, the Commissioner also made inspection visits to the device stores of the LEAs for the following purposes, namely,

(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 see the items that were outside the knowledge of the Commissioner or his staff and seek explanation as to how they might be used for conducting covert surveillance operations.

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

Removable storage media

3.28 To better control the issue and return of surveillance devices, the majority of the LEAs have adopted the computerised device management system ('DMS') in their device stores. My predecessor considered that the DMS was very useful in reducing human errors and keeping track of the movement of devices. I agree. During the last quarter of 2012, I advised the LEAs that the removable storage media for surveillance devices should be handled in a secure and strictly regulated manner akin to the withdrawal and return of surveillance devices so as to avoid any possibility of these storage media (e.g. memory cards, discs and tapes) being substituted, or in any way tampered with. This would also enable the LEAs to establish a proper chain of evidence in the event that the information obtained in the course of the surveillance was required as evidence in court. The LEAs have indicated that they will implement my recommendations. I have also suggested that the LEAs should ultimately use the DMS to record the issue and return of the removable storage media. This is currently being considered.

[This page is left blank.]

CHAPTER 4

DEVICES FOR NON-ICSO PURPOSES

Devices used for non-ICSO purposes

4.1 According to the ICSO, surveillance carried out without using any devices does not fall within the definition of 'covert surveillance'. Hence, tight control and close scrutiny have to be exercised over all surveillance devices capable of being used for covert surveillance under the Ordinance (i.e. capable devices) although they may be used by the LEAs for purposes which are not related to ICSO ('non-ICSO purposes'). This is to obviate the possibility that capable devices might be used for covert surveillance without authorization or even unlawfully. Therefore, apart from keeping track of surveillance devices used for ICSO purposes, it is also necessary to monitor the movement and use of capable devices, albeit they may allegedly be used only for non-ICSO purposes such as using a digital camera to take photos of a crime scene, etc. As a matter of practice, an authorized covert surveillance is always supported by a prescribed authorization issued by a relevant authority which makes checking simpler, but a surveillance claimed to be for non-ICSO purposes will not have that support. This necessitates the making of enhanced requirements when devices are drawn out for non-ICSO purposes than for ICSO purposes.

4.2 The requirements that have been accepted by the LEAs are that for the issue of surveillance devices without the support of a prescribed authorization, which cannot be for the purpose of carrying out covert surveillance under the ICSO, for example, overt surveillance

at a public place, a two-level approval by way of an endorsement of an officer ('the endorsing officer') and an approval of a senior officer ('the approving 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 ('the issuing officer') will issue the surveillance devices requested.

Cases brought forward from Annual Report 2011

4.3 There were three outstanding cases in the Annual Report 2011 and progress of the cases is set out in the ensuing paragraphs.

Outstanding Case (i): Duplicate use of request memo reference [Paragraphs 4.4 to 4.37 of Annual Report 2011]

4.4 There were four cases of duplicate use of device request memo reference and mistakes in the names of endorsing officer and approving officer in the device register which were discovered in April 2010. The LEA attributed the repeated anomalies and irregularities unearthed to inadvertent oversight and carelessness of the officers concerned and the difficulties they encountered in adapting to the new requirements for withdrawal of devices. The remedial action taken by the LEA was to remind the officers concerned to exercise greater care in handling the device register and request memo. As certain officers had failed to perform their responsibilities as expected of their respective post and rank and should be subject to a higher level of discipline, the LEA was requested to conduct a review and submit its recommendation on the proposed disciplinary actions to be taken against the officers concerned.

4.5 Taking into account the nature/frequency of procedural impropriety or supervisory oversight involved, the LEA proposed that counselling (non-disciplinary in nature) be given to the following officers:

(a) the approving officer in Case 2;

(b) the endorsing officer in Case 3 who was also the approving officer in Case 4;

(c) the officer-in-charge of the device registry concerned;

(d) the withdrawing officer who used a wrong name chop to chop the name of the endorsing officer in the device register when drawing devices for an operation; and

(e) the issuing officer who did not detect the mistake mentioned in (d) above.

4.6 The LEA explained that as far as counselling was concerned, this type of sanction did provide some measure of deterrence because a permanent record would be placed in the officers' personal record and reflected in performance assessments. In view of this explanation and having considered the precedents where counselling had been deemed appropriate in the LEA, I raised no objection to the proposed actions against the officers concerned.

Outstanding Case (ii): Alleged input problem of the DMS [Paragraphs 4.68 to 4.97 of Annual Report 2011]

4.7 This case was discovered in March 2011 when the DMS failed to record the return of a camera ('camera 006') because of an "input problem" as alleged by the LEA. My predecessor completed a review on most of the matters relating to this case and his findings were

set out in Annual Report 2011. For the outstanding matters as to whether the storekeeper concerned ('Storekeeper') and the Sub-administrator of the device registry ('the Sub-administrator') had given false statements, a separate investigation was conducted by the LEA ('the investigation'). In March 2013, the head of the LEA submitted to me a report on the findings of the LEA's investigation ('the investigation report').

Second attempt to process the return of camera 006

4.8 When camera 006 and the other two devices issued under a different device request memo were returned to the device registry and processed in a single return process in the DMS, the system did not accept the return of camera 006 because of the system design. According to the Storekeeper, he logged out from the DMS and logged in the DMS again to retry the return process of camera 006 ('the second attempt'), which was, he believed, completed successfully. However, the checking of system logs by an engineer about ten days later could not locate any log relating to the successful return of camera 006. This called into question as to whether the Storekeeper had actually made the second attempt as claimed by him.

4.9 When interviewed during the investigation, the Storekeeper insisted that he had made the second attempt and was sure that he had successfully finished the return process for camera 006 as the display on the DMS screen was no different from the normal successful transaction. For the system log check by the engineer, the investigation report stated that when checking the system logs, the engineer was not focusing to check against every step taken by the Storekeeper in the DMS and she was, therefore, not aware of whether there were any system logs regarding the relog-in or retry on the return of camera 006 by the Storekeeper. The system logs concerned had

already been overwritten as preset in the system and could no longer be retrieved after the lapse of time. In sum, there was no evidence to disprove the statement of the Storekeeper. On the other hand, the officer who returned camera 006 to the device registry ('the Returning Officer'), on the basis of his observations on the actions taken by the Storekeeper at the material time, believed that the Storekeeper had re-logged into the DMS to retry the return process for camera 006. The LEA concluded that there was no evidence to show that the Storekeeper had made a false statement and that there was no apparent incentive for him to make a false statement.

Notification of the result of the system log check by the engineer

4.10 According to the information provided by the engineer to my office during my predecessor's review on this case, the engineer had checked the system logs after being approached by the Sub-administrator regarding the "input problem" and then informed the Sub-administrator of the checking result. However, the Sub-administrator stated that he did not know that the engineer had checked the system logs and she had never told him any information about the checking result. On the face of it, there was a contradiction in the statements given by the engineer and the Sub-administrator.

4.11 The LEA interviewed the officers concerned with a view to investigating whether the Sub-administrator had given a false statement in this regard. The investigation findings revealed no witness or other first-hand evidence to support or disprove either the Sub-administrator's or the engineer's versions and there was, therefore, no evidence to disprove the statement of the Sub-administrator. From all the information provided by the engineer, the LEA could not find any exchange of information between the Sub-administrator and the engineer revealing that the

Sub-administrator should have clearly received the engineer's message of the system log check result and in return have provided his feedback accordingly. The LEA considered that there was doubt as to whether the Sub-administrator had actually received the engineer's message of the system log check and the relevant result, if it existed. In addition, given the Sub-administrator's role which was independent from the Storekeeper and the Returning Officer, the LEA did not see the need for him to deny having been informed by the engineer about the system log check result, if he was so informed. In sum, the LEA concluded that there was no evidence that the Sub-administrator had made a false statement.

Alleged input problem

4.12 The investigation report stated that after the Sub-administrator had scrutinised the reports by different officers concerned and having considered that there had been no finding that the Storekeeper had not properly completed all return procedures for camera 006 in DMS, the Sub-administrator accepted that there was an "input problem" of DMS when the Storekeeper was handling the return procedures for camera 006. The LEA considered that it was not an unreasonable conclusion for the Sub-administrator as a layman to draw based on what he understood at that time, including the fact that DMS did not accept the successful return of camera 006 in a single transaction because it was issued under a different device request memo.

Counselling on the Sub-administrator and the Storekeeper

4.13 The LEA concluded to the effect that there was no or no sufficient evidence upon which it could draw a conclusion that either officer had acted dishonestly in respect of their involvement in the

incident and the subsequent investigation. However, the LEA considered that both officers had definite room for improvement on their alertness and sensitivity and proposed that a strong counselling (non-disciplinary in nature) be administered on them.

Remedial/improvement measures

4.14 Apart from conducting more seminars to reinforce knowledge, promote awareness and imbue a prudential mindset, the LEA would install new facilities to ensure that officers could acquire hand-on experience of using DMS beforehand. The DMS was also enhanced so that it could retain an audit trail for an extended period.

Review by the Commissioner

4.15 Having considered the investigation report submitted in March 2013, I agreed to the proposed actions against the Sub-administrator and the Storekeeper. The remedial/improvement measures that would be/had been taken by the LEA were also considered appropriate.

Outstanding Case (iii): Discrepancies regarding the time of making retrospective entries of the issue of devices for non-ICSO purposes in the relevant register of the DMS, the manual records and the DMS audit log [Paragraphs 4.99 to 4.102 of Annual Report 2011]

4.16 The case was reported by the LEA in December 2011. The LEA stated in its investigation report submitted in March 2012 that at about 0945 hours on a certain day in April 2011, the officer-in-charge of a non-ICSO operation ('OC Operation') was informed that the operation of the DMS would be suspended for scheduled maintenance. The OC Operation obtained at 1130 hours verbal approval from the Supervisor who was on leave via telephone for issuing five devices (i.e. Devices (a)

to (e)) to be deployed in the operation. The OC Operation then instructed his subordinate to make a manual record of the issue of the said devices. According to the relevant entry of the manual record ('the Entry'), Device (d) was issued at 1139 hours.

4.17 When the operation of the DMS resumed, the OC Operation obtained a password from the Supervisor at 1609 hours and commenced the retrospective input of the issue of the devices into the DMS. He also instructed his subordinate to make a manual record of the retrospective input, which read 'The written records of the Entry were retrospectively inputted to DMS at 16:10 today'.

4.18 The OC Operation made two mistakes during the retrospective input of Device (d). First, '1610' (hours) was wrongly input as the 'Retrospective Issue date/time' which in fact should be 1139 hours as shown in the manual record. Second, '1609' (the time when the password was obtained from the Supervisor) was wrongly input as the 'Approval date/time' which in fact should be the time when the verbal approval of the Supervisor was obtained at 1130 hours. Similar mistakes were made in the retrospective input for Device (e).

4.19 Upon completion of the retrospective input for Device (e), the OC Operation realised that he had made mistakes concerning the 'Retrospective Issue date/time'. He ceased making further inputs and informed the Supervisor of the problem who decided to return to the office to deal with the matter. At about 1800 hours, the Supervisor returned to the office and decided to deal with the retrospective inputs in respect of Devices (a), (b) and (c) first. According to the DMS audit log, the input processes were completed at 1829 hours, 1833 hours and 1831 hours. During the process, the OC Operation was advised by the Supervisor to enter '18:27', '18:32' and '18:30' as the time of making the retrospective inputs for Devices (a), (b) and (c) respectively under

the 'Remarks' column of the DMS. The Supervisor later revised the wording of the OC Operation's inputs under the 'Remarks' column. In particular, he altered the time of making the retrospective inputs for Devices (a), (b) and (c) respectively to '16:13', '16:14' and '16:15'. It was apparent that these amendments had the effect of changing the records from accurate to inaccurate.

4.20 The OC Operation accepted full responsibility. He was apologetic for his mistakes and accepted that he should have been more vigilant and conversant with the requirements when making retrospective inputs into the DMS. He had promptly reported his mistakes to the Supervisor. The Supervisor also accepted full responsibility for entering the wrong time of making retrospective inputs. He asserted that his mistakes were unintentional and accepted that he should have been more vigilant when editing the contents of the entries.

4.21 The LEA attributed the irregularity to the inadequate vigilance by the Supervisor and the OC Operation. It recommended that an advice (non-disciplinary in nature) be given to the OC Operation on the need to ensure that all information required for making inputs into the DMS must be accurately entered into the DMS and to be fully conversant with the requirements for operating the DMS, and a verbal warning be given to the Supervisor for the mistakes concerning the time of making retrospective inputs.

4.22 I considered that there was no evidence of misconduct on the part of the officers and that the proposed disciplinary actions were appropriate.

Cases occurring or discovered in 2012

4.23 In 2012, reports from the LEAs on five cases relating to devices for non-ICSO purposes were received. Details of these cases are described below.

A. Discrepancies of records relating to withdrawal and return of devices

4.24 At an inspection visit to an LEA in December 2011, the device registers of the LEA were examined and some questions on the information contained in the registers, including the name/post of concerned officers and the approval date for withdrawal of the devices, were raised. Upon request, the LEA submitted an investigation report in February 2012 setting out the explanation and/or clarifications on the discrepancies of records in the registers in relation to the withdrawal and return of devices.

4.25 The LEA concluded that the discrepancies found in the entries of the device registers were errors made by individual officers and there was no misconduct, malpractice or improper behaviour involved. The officers concerned had been counselled and reminded to be more careful in checking the accuracy and completeness of the information on the device request memo and the device register. The LEA had taken improvement measures to address the issue. I accepted the LEA's conclusion and considered the improvement measures appropriate.

B. False report by a storekeeper in respect of the reason for no DMS record of return of devices

4.26 In mid March 2012, an LEA submitted an initial report on an incident where the DMS failed to record the return of three surveillance devices ('the three devices') due to power failure.

The account given in the initial report

4.27 On a certain Saturday morning in March 2012 ('the relevant date'), a device storekeeper ('Storekeeper') issued 11 surveillance devices to four team leaders for conducting a non-ICSO operation. Three of these devices were issued to one of the four team leaders ('Team Leader A'). When the operation ended in the afternoon, the team leaders returned to the device store concerned. The Storekeeper recorded in the DMS the return of eight surveillance devices from the three team leaders who first returned to the device store. When Team Leader A returned to the device store, the power supply of the device store broke down. As the DMS could not be operated, the Storekeeper recorded the return of the three devices by Team Leader A in a manual non-ICSO device register instead. This version of the incident was given by the Storekeeper.

4.28 On the next Monday morning, the Storekeeper reported the incident to his supervisor ('Supervisor') who instructed the Storekeeper to make a retrospective entry into the DMS. However, the Storekeeper mistakenly used the normal return function instead of the function of retrospective entry, resulting in an incorrect record showing that the three devices were returned only on Monday instead of the relevant date. This wrong entry was discovered two days later during a weekly inspection.

Progress reports and full investigation report submitted by the LEA

4.29 The DMS terminal had been examined twice by the engineer and there was no evidence of any power failure on the relevant date. The LEA was informed of the examination result by the engineer in early April 2012. In mid April, the LEA wrote to the Secretariat to advise the results of the examination of the DMS terminal. The LEA stated that it would appear that the initial version as given by the Storekeeper 'might not be entirely true' and an independent investigation would be conducted into the matter.

4.30 In mid May 2012, the LEA formally advised the Secretariat that the Storekeeper admitted that he had made up the story of a power failure to cover up his failure to make a proper return record of the three devices.

4.31 The LEA submitted a full investigation report in September 2012 and provided further information in November 2012.

False report by the Storekeeper

4.32 During an interview in end March 2012, the Storekeeper confessed that he had made a false report of a power failure to cover up his negligence in not recording the return of the devices in the DMS. On the date of the incident, after recording the return of the eight surveillance devices from the three other team leaders, he decided not to wait for Team Leader A but to conduct a debriefing with the teams regarding the non-ICSO operation. When the Storekeeper was about to leave the device store and proceed to the debriefing, Team Leader A arrived with the three devices. The Storekeeper told her to leave the devices on a table in the device store and that they would process the return of the devices through the DMS afterwards. After the

debriefing, the Storekeeper returned to the device store, locked up the returned devices and went off duty. Both the Storekeeper and Team Leader A had forgotten that the return of the three devices had not been properly recorded in the DMS. On the next Monday, the three devices were required to be issued but the request was rejected by the system because the DMS record showed that they had yet to be returned. At that time, the Storekeeper realised that he had forgotten to record the return of the devices in the DMS. He reported to his Supervisor that the return of the three devices was not properly recorded in the DMS. When asked by the Supervisor for the reason, he made up the excuse that there was a power failure in the device store.

LEA's findings and proposed disciplinary actions

4.33 After investigation, the LEA concluded that the Storekeeper had failed to record the return of the three devices in the DMS due to negligence and that he had made up the account of a power failure to cover up his mistake. While Team Leader A had also failed to return the three devices through the DMS due to negligence, there was no evidence to show that she knew about the making of the false report by the Storekeeper. The LEA was conducting a disciplinary review to determine the appropriate disciplinary charges to be laid against the Storekeeper and Team Leader A.

4.34 For the Supervisor, the LEA considered that she had not taken necessary actions to verify the report of power failure made by the Storekeeper. She had also failed to take appropriate follow up action to check if proper retrospective return records had been made as instructed by her. The LEA proposed that the Supervisor be given a verbal warning. I considered the proposed disciplinary action appropriate.

Review by the Commissioner

4.35 In reviewing the handling of this case, I was very concerned about the LEA's prevarication in not immediately advising the Secretariat of the true position. The facts revealed that the Storekeeper had confessed in late March 2012 about fabricating the account about a power failure preventing his making of a proper return record of the devices; and by early April 2012, this had been confirmed by the two examinations of the DMS by the engineer. In the circumstances, the Secretariat should have been advised of these facts at the earliest opportunity. It was noted with regret that the LEA wrote to the Secretariat in mid April 2012 stating that '*It would appear that the initial version as given by the device store keeper … may not be entirely true'*. This was unquestionably misleading. The account given by the Storekeeper was entirely false, it was a deliberate fabrication and this was known to the LEA when it wrote to the Secretariat. While the LEA had explained that it considered it more appropriate to have the facts fully verified before its inclusion in the written submission to the Secretariat, I did not find this to be a reasonable excuse.

4.36 Another matter which concerned me was that the LEA did not take a statement from the Storekeeper immediately after his confession at an interview in late March 2012 but only did so three weeks later. Even then, the Secretariat was not advised of the Storekeeper's confession until May 2012 i.e. six weeks after the true situation was known to the LEA.

C. Use of a personal mobile phone by an LEA officer to take a photograph in an observation

4.37 An LEA first reported in June 2012, followed by an investigation report in August 2012 on the use of a personal mobile phone by an officer ('the Officer') to take a photograph in a non-ICSO operation.

4.38 Investigation from the LEA revealed that in January 2012, the Officer conducted an observation to gain information pertaining to an investigation. According to the DMS, no non-ICSO devices had been issued for the purpose of this observation. It was revealed that during the operation, the Officer took a photograph of some objects with his personal mobile phone and the photograph was subsequently mentioned in a debriefing session. According to the legal advice, the incident did not involve any covert surveillance as defined in section 2 of the ICSO and therefore did not constitute non-compliance with the ICSO. The LEA considered that the Officer's conduct in this case had compromised the intended function of the control of devices through the DMS and was in breach of its internal requirement. In this regard, the LEA recommended that a verbal warning be given to the Officer. The LEA had also issued a reminder to its officers of the need to strictly adhere to the requirement that only officially issued devices should be used in discharging operational duties.

4.39 Having reviewed the case, I agreed that the unsatisfactory conduct of the Officer did not constitute non-compliance with the ICSO and the proposed disciplinary action was appropriate.

D. Wrong staff number of an officer recorded in a non-ICSO device register

4.40 When a senior officer conducted a monthly inspection, he discovered that the staff number of an officer was mistakenly recorded in 11 entries of a non-ICSO device register during a period of about ten days. Two of the digits of the staff number were transposed. In these entries, the officer concerned was an officer who withdrew/returned devices from/to a device registry ('Withdrawing/Returning Officer').

4.41 The procedures and practices adopted by the LEA for drawing and returning of surveillance devices prevailing at the material time are set out below:

(a) Only designated officers would be allowed to withdraw/return surveillance devices from/to a device registry.

(b) A user account for the designated officer would be created in the DMS, which contained his/her personal information including name, warrant card number, staff number, etc.

(c) When withdrawing/returning devices, the designated officer should present to the issuing/receiving officer his/her warrant card for verification of his/her identity. The issuing/receiving officer would input into the DMS the warrant card number of the designated officer shown on the warrant card. The device issue/return process could proceed further only when the warrant card number entered was accepted by the DMS. The designated officer's personal information as stored in his/her user account would be shown in the DMS terminal for the checking of the issuing/receiving officer.

(d) After completion of the device issue/return process, the issuing/receiving officer would print a Record of Issue/Return stating, inter alia, the name, warrant card number and staff number of the designated officer as stored in his/her user account.

(e) The designated officer was required to sign on the Record of Issue/Return to confirm the withdrawal/return of the devices, which would then be provided to the officer who approved the request for withdrawal of the devices ('Approving Officer').

Cause of the errors

4.42 According to the investigation report submitted by the LEA, the errors in the device register were due to the wrong information provided by the supervisor of the Withdrawing/Returning Officer for the creation of a DMS user account for the Withdrawing/Returning Officer. The supervisor mistakenly transposed two of the digits of the staff number of the Withdrawing/Returning Officer.

Failure to detect the errors

4.43 For the 11 wrong entries, a total of six issuing/receiving officers were involved. They did not detect the incorrect staff number of the Withdrawing/Returning Officer when processing the withdrawal/return of devices by the Withdrawing/Returning Officer through the DMS. The errors were not detected by the Withdrawing/Returning Officer when signing on the relevant Records of Issue/Return. The Approving Officer concerned was also unable to detect the errors from the copies of the Records of Issue/Return provided to him. The head of the device registry concerned was

required to conduct weekly inspections of the device registry but failed to discover the errors during the inspection.

Action taken against the officers concerned

4.44 The investigation report stated that the concerned officers would be reminded to be more careful in performing their duties. In response to my request for re-consideration of the actions that should be taken against individual officers, the LEA proposed to administer counselling (non-disciplinary in nature) on two officers and issue a stern reminder to other officers concerned. According to the LEA, since a permanent record of counselling would be placed in an officer's personal record and suitably reflected in subsequent performance assessments, this kind of sanction would provide some measure of 'cautionary effect'. The two officers who would be given counselling were the head of the device registry concerned who overlooked the accuracy of the staff number when checking records of the device registry during weekly inspection and an issuing/receiving officer who failed to spot the incorrect staff number when processing the withdrawal/return of devices by the Withdrawing/Returning Officer on a total of six occasions.

Remedial/improvement measures

4.45 The incident revealed certain inadequacies of the DMS and the device issuing/returning procedures of the LEA. In this connection, the LEA had taken or would take the following remedial/improvement measures, of which items (b) and (c) were proposed by the LEA in response to my observations raised during my review of the incident:

(a) To ensure the accuracy of the information input into a DMS user account, a new procedure was put in place that required the user to visit the device registry with his/her warrant card for checking before a user account was created.

(b) To minimize the risk of human errors in the course of the input of data for creation of a DMS user account and verification of the identity of a user in the process of issue/return of devices, the LEA would adopt an automatic card reading method whereby the required information stored in the warrant card would be captured from the card by a card reader automatically.

(c) To remedy the loophole whereby the devices could be withdrawn on any day after approval of the request for withdrawal of devices was obtained, the device request form was revised to add an indication on when the devices would be withdrawn.

The Commissioner's findings

4.46 While agreeing to the proposed actions to be taken against the officers concerned and the proposed remedial/improvement measures, I have reminded the head of the LEA that there needed to be a change in the attitude of the officers who were involved in the registration and control of the movement of surveillance devices. The mistakes involved in this incident and previous cases relating to the device-recording system of that LEA were plainly due to the carelessness, inattentiveness or complacency on the part of the officers concerned, which was a matter required to be addressed. It was imperative that the officers should ensure the accuracy and integrity of

the records of the device registries. I recommended that the LEA should address this issue and in particular to instil in concerned officers the need for strict adherence to the requirements for the management of capable devices and that those who did not adhere to these objectives should not be deployed in this area.

E. Improper record on redeployment of devices

4.47 On a certain day in October 2012, 15 surveillance devices were issued for conducting a non-ICSO operation. However, it was decided in the afternoon that these devices would be redeployed to another non-ICSO operation ('the new operation'). After the new operation concluded later on the same day, the surveillance devices were returned to the device store. According to the established procedures of the LEA concerned, the device storekeeper should make a record in the DMS on the redeployment of surveillance devices to the new operation before processing the return of them through the DMS. In this case, the device storekeeper forgot to make a record in the DMS on the redeployment of the 15 surveillance devices to the new operation. He realised this mistake only after making the return record for the 15 surveillance devices. He immediately reported the incident to his supervisor and admitted his fault.

4.48 The supervisor then informed the officer-in-charge of the surveillance unit concerned of the incident, who instructed the device storekeeper to make retrospective issue and return records in DMS in respect of the 15 surveillance devices for the new operation and to make remarks on the relevant DMS entries about the redeployment of devices from one operation to another operation. After investigation, the LEA concluded that there was no evidence of malicious act or ulterior motive. The device storekeeper was reminded to be more vigilant in handling capable devices and follow proper procedures in the

control of capable devices. The LEA reported the incident and the results of its investigation to the Secretariat six days later.

4.49 I accepted the LEA's conclusion and agreed to the action taken against the device storekeeper. In addition, I commended the LEA for the way that this incident had been handled including the prompt and frank reporting by the device storekeeper upon his discovery of his mistake, the appropriate remedial actions taken by his supervisors and the swift follow up actions taken by the LEA in investigating and reporting the incident.

[This page is left blank.]

CHAPTER 5

LEGAL PROFESSIONAL PRIVILEGE AND JOURNALISTIC MATERIAL

Obligations of LEAs regarding LPP cases

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

5.2 Paragraph 121 of the COP provides that the LEA should notify the Commissioner of interceptions/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.

5.3 Regarding 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 likelihood of obtaining LPP information. If subsequently there is anything that transpires which may affect the assessment, which is considered as a material change of circumstances, the LEA has to promptly notify the panel judge of the altered LPP assessment by way of an REP-11 report. The LEA has to provide the details of all relevant circumstances, including as to 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 its officers have taken or propose 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 LEAs would also give the Commissioner a similar notification of each of such occurrences.

5.4 The panel judges continued to be very cautious in dealing with cases that might possibly involve LPP information being obtained by an LEA. When it was assessed that there was such likelihood and if they granted the authorization or allowed it to continue, they would impose additional conditions. These additional conditions obliged the LEA to report back when the likelihood was heightened or when there was any material change of circumstances so that the panel judge would reconsider the matter in the new light. These additional conditions were stringent and effective in safeguarding the important right of individuals to confidential legal advice.

The Commissioner's requirements to the LEAs

5.5 There is a set of reporting and preservation requirements when an LEA encounters a call with LPP likelihood, heightened LPP likelihood or LPP information. The LEA is required to submit an REP-11 report to the panel judge on this call. This is named a '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, 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 state 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. The LEA should preserve the interception products of all intercepted calls when such products are still available at the time of discovery of the Reported LPP Call, the transcripts, summaries, notes, ATRs, etc. The preserved records should not be destroyed without the prior consent of the Commissioner. Similar arrangements should also be made in respect of cases where journalistic material ('JM') is involved or likely to be involved.

LPP reports received in 2012

5.6 In the report period, there were 13 LPP cases with submission of REP-11 reports to the panel judges. They included:

(a) one case of obtaining information subject to LPP; and

(b) 12 cases of heightened likelihood of obtaining LPP information.

5.7 In the first case, the interception operation was not assessed to have a likelihood of obtaining LPP information at the grant of the prescribed authorization for interception. As the interception progressed, one day, after listening to part of a call, the listener formed the view that information subject to LPP had been obtained and she

immediately reported the matter to her supervisor who directed that the monitoring should be suspended. The LEA then submitted an REP-11 report to the panel judge and sought approval to resume the monitoring. After considering the REP-11 report, the panel judge allowed the prescribed authorization to continue with additional conditions imposed to guard against the risk of obtaining LPP information. On the same day that the monitoring of the operation resumed, the listener listened to part of an intercepted call from another telephone number and formed the view that LPP information had been obtained and reported the matter up the chain of command. An REP-11 report and a discontinuance report were subsequently submitted to the panel judge who duly revoked the prescribed authorization.

5.8 For the other 12 LPP cases, the interception operations were not assessed to have a likelihood of obtaining LPP information at the grant of the prescribed authorizations for interception. The LEAs formed the view in the midst of interception operations that there was a heightened likelihood of obtaining LPP information through continued interception. REP-11 reports and discontinuance reports were subsequently submitted to the panel judge who revoked the authorizations.

5.9 In the review of LPP cases, I together with my staff or my predecessor have checked all the relevant documents and records including the prescribed authorization, the REP-11 report, the determination by the panel judge, the listener's notes, the written summaries, the call data, the ATRs, etc. It was also checked whether the LEA 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 written summaries passed on to

investigators, whether there were calls between the same telephone numbers preceding the Reported LPP Call that should have been but had not been reported to the panel judge, and whether there was any listening or re-listening to the interception product after the discontinuance or revocation of the prescribed authorization.

5.10 Pending a decision by the Administration on the issue regarding the power of the Commissioner to listen to the recording of interception products, there was no recording of intercepted calls listened to in the review of LPP cases in 2012. Hence, no finding could be made as to the veracity of the content of the conversations in the Reported LPP Call as stated in the REP-11 reports. Similarly, no finding could be made as to whether the calls preceding the Reported LPP Call also had LPP information or likely LPP information or increased LPP likelihood that ought to have been reported to the panel judge in the first instance, or whether there were any communications subject to LPP other than those reported. Subject to these qualifications, nothing untoward was found in any of these cases.

Outstanding LPP case in 2011

5.11 It was reported in paragraph 5.65 of the Annual Report 2011 that the head of an LEA had been asked to consider what action he proposed to take against the officers concerned with the unsatisfactory handling of an LPP case. Briefly, no REP-11 report had been made to the panel judge and there was no genuine effort to check the number of 'other calls'. The LEA had provided a figure of eight but subsequently the Secretariat found that there were in fact 26 calls when the archived data was checked. The LEA replied that an officer would be verbally advised, with a record on file, of the importance of verifying the accuracy of information before passing the same to the Commissioner

or his staff. The advice was disciplinary in nature. In addition, relevant officers working on ICSO-related duties were reminded of the requirement to submit an REP-11 report, together with a discontinuance report if the LEA decides to discontinue the operation, in relation to the listening of Reported LPP Calls. My predecessor noted and did not raise objection to these actions.

Obligations of LEAs regarding JM cases

5.12 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.

JM reports received in 2012

5.13 In the report period, the Commissioner received three reports of JM cases. They included:

(a) one case where it was assessed that there was a likelihood of obtaining JM through interception of the facility; and

(b) two cases of heightened likelihood of obtaining JM.

5.14 In the first case, the interception operation was assessed to have a likelihood of obtaining JM at the time of the application for authorization. When granting the prescribed authorization, the panel

judge imposed a set of additional conditions requiring the LEA to report to the panel judge upon detection of any JM.

5.15 On one occasion, the listener listened to part of an intercepted call and formed the view that continued listening to the subject facility might inadvertently obtain JM. She suspended the monitoring immediately. An REP-11 report and a discontinuance report were subsequently submitted to the panel judge. The panel judge revoked the authorization.

5.16 For the other two JM cases, it was not envisaged that the interception operations would likely involve JM at the time of applying for authorization. During these operations, when the listeners formed the view that continued listening might inadvertently obtain JM, they suspended the monitoring immediately. REP-11 reports and discontinuance reports were subsequently submitted to the panel judge. The relevant prescribed authorizations were duly revoked by the panel judge.

5.17 I conducted a review of these three JM cases. No irregularity was found. However, as I had not listened to the interception products, no findings could be made as to the veracity of the contents of the calls as stated in the REP-11 reports and whether apart from those calls, there were any other communications which might have contained JM in the interception products listened to by the LEA.

[This page is left blank.]

CHAPTER 6

APPLICATION FOR EXAMINATION AND NOTIFICATION TO RELEVANT PERSON

The law

6.1 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 departments. 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.

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/her by the Government.

6.2 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) 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) 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

6.3 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/her 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.

The applications under section 43

6.4 During the report period, a total of 18 applications for examination were received, one of which could not be entertained because the application had not raised matters within the ambit of the function of the Commissioner. Another six applications were subsequently not pursued by the applicants. Of the remaining 11 applications, four alleged interception, one suspected covert surveillance and six claimed a combination of interception and covert surveillance. Since none of the 11 applications came within the ambit of the exceptions covered by section 45(1), the Commissioner carried out an examination provided for in section 44 in respect of each case.

6.5 After making all necessary enquiries, I or my predecessor found all these 11 cases not in the applicants' favour and accordingly notified each of the applicants in writing of the finding relating to him/her, with five of such notices issued during the report period and six 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.

Applications affected by section 45(2)

6.6 In 2012, there was no application subject to section 45(2) of the Ordinance.

Notification to relevant person under section 48

6.7 Section 48 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.

6.8 Consideration of the application of section 48 may arise under a number of situations. For example, the interception of telephone communications through the use of a telephone number other than that permitted by a prescribed authorization issued by a panel judge, however that error is made, constitutes an unauthorized interception. It gives rise to the necessity of considering whether the Commissioner should, as obliged by section 48 of the Ordinance, give a notice to the relevant person of the wrong interception and invite him/her to make written submissions in relation to the assessment of reasonable compensation to be paid to him/her by the Government.

6.9 In processing cases under section 48, my predecessor had taken into consideration the following non-exhaustive factors in assessing the amount of compensation that the Government should properly pay to the relevant person:

(a) the duration of the interception and/or covert surveillance;

(b) the number of the communications that had been intercepted or the extent of the conversations and activities that had been subject to covert surveillance;

(c) the total duration of the communications, conversations or activities that had been intercepted or subject to covert surveillance;

(d) the sensitivity of the communications, conversations or activities;

(e) injury of feelings such as feelings of insult and embarrassment, mental distress, etc;

(f) whether the unauthorized act was done deliberately, with ill will or ulterior motive, or done unintentionally and resulted from negligence, oversight or inadvertence; and

(g) the degree of the intrusion into privacy in the context of the number of persons outside the communications, conversations or activities having knowledge of the contents, whether such persons would remember or likely remember their contents, and whether such persons know the relevant person and the other participants to the communications, conversations or activities.

6.10 The written submissions made by the relevant person, which may involve any or all of the above factors, will be considered for making the assessment.

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

Elaboration on the application requirements

6.12 A number of applicants and complainants did not understand the basis of an application for examination under the Ordinance. It is only when the proper basis of an application is satisfied that the Commissioner is entitled to institute the process of examination of the case. The proper basis is to satisfy both of 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.

6.13 Regarding requirement (a), one common complaint was that the complainant was 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 were complaints of either the complainant being implanted with a device that could read and manipulate his/her mind or being tracked and injured by rays emitted by a device. These again do 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.

6.14 Regarding requirement (b), some applicants described how a particular person, as opposed to an LEA officer, carried out the suspected interception or covert surveillance. This failed to satisfy this second requirement to entertain an application or to engage in an examination.

6.15 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, there are leaflets available to prospective complainants which contain the necessary information for making an application.

Statutory prohibition against disclosure of reasons for determination

6.16 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.

6.17 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.

[This page is left blank.]

CHAPTER 7

REPORTS OF NON-COMPLIANCE, IRREGULARITIES AND INCIDENTS

Reporting of non-compliance, irregularities and incidents

7.1 By virtue of section 54, where the head of any department considers that there may have been any case of failure by the department 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). 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.

7.2 The section 54 obligation only applies where the head of the LEA considers that there may have been a case of non-compliance. The LEAs are also required to report cases of irregularities or even simply incidents to the Commissioner for his consideration and scrutiny so that any possible non-compliance will not escape his attention. Such reports are *not* made under section 54 of the Ordinance.

7.3 Some cases of non-compliance, irregularity or incident were discovered upon examination of the documents and information provided during inspection visits. In these circumstances, the LEA concerned is required to investigate the matter and submit a report to the Commissioner.

7.4 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.

Cases brought forward from Annual Report 2011

7.5 In the Annual Report 2011, there were two outstanding cases, the review of which has been completed. They are dealt with in the paragraphs below.

Outstanding Case (i): 893 instances of non-compliance with the Revised Additional Conditions imposed by panel judges in prescribed authorizations for interception [Paragraphs 7.189 to 7.237 of Annual Report 2011]

7.6 The nature of non-compliance was a breach of the revised additional conditions imposed by the panel judge in the prescribed authorization for interception to guard against the risk of obtaining LPP information. The three concerned officers were culpable because of their failure to obtain verification of their understanding or interpretation of the revised additional conditions (which as it transpired was incorrect) and the unsatisfactory manner in which they sought clarification from the PJO. The outstanding issues were the disciplinary action against the officers and the culpability or otherwise of the LEA's management in the matter as the case might have been discussed in a meeting in July 2011 where the senior officers were present.

7.7 In its letter of June 2012, the LEA indicated that the investigation findings did not suggest that the senior officers should be held culpable in the case because matters pertaining to interception operations were handled by the operation teams and the said meeting

was not the forum to discuss these operation issues. Hence, a conclusion could not be drawn that the LEA's management and senior officers concerned should have appreciated the risk of non-compliance with the revised additional conditions and thus instructed either further and better clarification be sought from the PJO or the Commissioner's attention be drawn to the revised conditions without delay. My predecessor agreed with that opinion and had advised the LEA accordingly in July 2012.

7.8 In its report of October 2012, the LEA indicated that the proposed verbal warning for each of the three officers was a disciplinary action and would be taken into account by the management for promotion and appointment purposes.

7.9 Having conducted a review, I agreed to the finding of my predecessor that while the case had not been handled by the LEA officers satisfactorily, there was no evidence of ulterior motive or ill will on the part of the LEA management or any of the officers concerned. The non-compliance had not given rise to any intrusion into the privacy of the subjects concerned since the contents of the interception products had not been accessed by the LEA officers. I had no objection to the proposed verbal warning for each of the three officers.

Outstanding Case (ii): Retention by an LEA officer of documents suspected to be related to interception operations [Paragraphs 7.238 to 7.244 of Annual Report 2011]

7.10 The case was reported in November 2011 as a possible irregularity where an officer of the LEA ('the Officer') was found to have retained documents relating to interception operations conducted a few years earlier in respect of the investigation of a crime under the Officer's command. Some of these documents were suspected to be notes or copies containing intelligence and might constitute

interception products which are protected under the ICSO. The ICSO and COP require LEAs to make arrangements to ensure that protected products are destroyed as soon as their retention is not necessary. To fulfil this statutory requirement, the LEA put in place internal guidelines on the destruction of protected products. According to the LEA's internal guidelines, the documents in question should have been destroyed within one month after the conclusion of the relevant interception operations.

7.11 My predecessor advised the LEA in early 2012 that it was not advisable to start an investigation as the Officer was then awaiting a criminal trial.

7.12 The trial was subsequently concluded and the Officer was struck off the strength of the LEA. Having consulted my predecessor and obtained legal advice, the LEA started an investigation and submitted a report in December 2012. The investigation revealed that whilst on interdiction from duty resultant from a criminal investigation, the Officer handed over the work and office to another officer. Two boxes of documents kept in the Officer's former office were subsequently found to contain a bundle of documents relating to previous interception operations. The LEA concluded that the Officer had breached the destruction policy stipulated in the departmental guidelines whereby these documents should be returned to the department within one month after conclusion of the operation for destruction and the manner in which the documents had been kept was unacceptable. In view of the serious nature of the breach of the internal destruction policy committed by the Officer, the LEA indicated that had the Officer been in employment, the Officer would have been given a disciplinary action not below the level of a written warning

(disciplinary) for the misconduct. However, no action was recommended as the Officer no longer served in the LEA.

7.13 As a consequence of this incident, the LEA considered that there was a need to update its internal procedures to improve the control and safeguard of notes taken from interception operations. It has reminded all staff concerned of the need to strictly follow the destruction policy concerning interception operations, ensure the safe custody of all ICSO-related documents in their possession and destroy them when no longer required.

7.14 I have reviewed the case. The documents constitute protected products as defined under the Ordinance and should have been destroyed some years ago according to the LEA's departmental guidelines. I considered that this was not a case of 'non-compliance' because the LEA had issued guidelines to ensure that the destruction requirements under the ICSO and the COP were satisfied. The Officer's act was in breach of these departmental guidelines. As regards the LEA's suggestions on improvement in departmental procedures to control and safeguard the relevant documents, I considered these appropriate.

Cases occurring in 2012

7.15 In 2012, the Commissioner received from LEAs reports of irregularities/incidents relating to ten ICSO cases. All were submitted *not* under section 54 of the Ordinance. They are dealt with in the ensuing paragraphs. Another five cases that related to the use of surveillance devices for non-ICSO purposes are covered in Chapter 4.

Report 1: Misinterpretation of a term used in the device request form

7.16 During an inspection visit to an LEA in February 2012, in the course of examining the review folder of a prescribed authorization for a Type 1 surveillance operation, it was found that although no device was issued on a certain day in November 2011, the acting officer responsible for vetting the device request form ('acting Vetting Officer') signed to confirm under the column 'Quantity issued' in the request form that one surveillance device was issued that day. The LEA explained that according to the vetting unit concerned, the heading 'Quantity issued' in the request form should mean 'Quantity to be issued'. As this was a distortion of the meaning of the term, the LEA was requested to provide a written explanation.

7.17 The LEA's investigation report submitted in March 2012 revealed that the vetting unit had adopted a practice whereby the device request form was signed by the vetting officer in the field 'Confirmed by:' under the column 'Quantity issued' before the actual issue of device(s). This practice was not in line with the purpose and meaning of the officer's confirmation under the column 'Quantity issued'. According to the acting Vetting Officer, after the assessment of whether the type and quantity of the device(s) sought were appropriate in the given operational circumstances, the post holder of the vetting officer would mark the quantity of each type of the device(s) to be issued under the column 'Quantity issued', and sign in the field 'Confirmed by:'. The substantive vetting officer ('Vetting Officer') also confirmed that this practice had been in place and he was unaware that the practice did not properly reflect the purpose and meaning of signing in the said field on the request form.

7.18 The LEA submitted a further report in May 2012 to explain why the senior officers, i.e. the supervisor of the Vetting Officer ('the Supervisor'), the Assistant Head of Department and the Reviewing Officer failed to detect the mistake of the acting Vetting Officer when they reviewed the case. The LEA also stated that since 18 April 2012, the vetting officer would only append his signature in the field 'Confirmed by:' under the column 'Quantity issued' after the actual issue of the device. The LEA agreed that the literal interpretation of the term 'Quantity issued' meant the quantity of devices that had been issued and the practice adopted by the acting Vetting Officer was due to his misinterpretation of the purpose and meaning of the term. It recommended that a verbal warning (disciplinary) be given each to the Vetting Officer and the acting Vetting Officer for their failure to ensure that the device issuing procedure was in line with the meaning and purpose as required by the device request form, and a verbal warning (disciplinary) be given each to the Supervisor and the Assistant Head of Department for their failure to detect the mistake. For the Reviewing Officer, the LEA recommended that an advice be given to her as she had attempted a thorough review of the prescribed authorization.

7.19 Having conducted a review, I considered that there was no evidence of deliberate disregard of the procedures for the control of surveillance devices on the part of the five officers involved in this case. Regarding the proposed disciplinary actions against the acting Vetting Officer, the Vetting Officer and the Supervisor, since their respective failure to realise or discover the misinterpretation of the term 'Quantity issued' in the device request form was in part caused as a consequence of their following the then existing practice, I considered that an advice, instead of the proposed verbal warning (disciplinary), for each of them might be more appropriate and likewise that an advice, instead of the proposed verbal warning (disciplinary), to the Assistant Head of

Department might be more appropriate. The proposed advice to the Reviewing Officer was considered reasonable. The LEA has been advised accordingly.

Report 2: An incident in which a surveillance operation was discontinued but upon the return of surveillance devices, it was erroneously represented in the device register that the operation would still continue

7.20 The LEA submitted a report to the Commissioner in August 2012 to report an incident where a Type 2 surveillance operation was discontinued but upon the return of the devices which had been used in the operation, it was erroneously represented in the respective device register that the operation would still continue. After obtaining the authorization for a Type 2 surveillance operation, the case officer arranged to retrieve surveillance devices from the store on two occasions and these were then returned properly. On the third occasion, having considered that the expected results had been achieved, the case officer decided to discontinue the operation. When the devices were returned, the device receiving officer clicked the 'continue' button which automatically led to a 'No' being shown in the column of 'Reporting Discontinuance with Date' in the device register which was not correct.

7.21 The investigation revealed that the device receiving officer at the time was a relieving officer. He believed that if the operation was discontinued, the case officer would inform the device receiving officer on duty. The case officer claimed that he was not aware of the need to remind his officer to relate the message to the device registry when returning the devices. The LEA noted that there was a misunderstanding between the two officers and it recommended that all officers responsible for the device issuing/receiving duties, including those relieving officers, would be reminded to be more careful in

performing their duties. It was also determined that the case officer should make a timely notification of the state of operations at the time of the return of devices. As a short term remedial measure, it was proposed that the case officer should make personal call to the device receiving officer on duty each time there was a return of devices and state the status of the operation. The oral notification should be followed by a written confirmation. As a long term measure, the LEA recommended to use a device return form each time when devices were returned to avoid any ambiguity as to whether the operation would continue or not.

7.22 At an inspection visit to the LEA in December 2012, I examined the documents in connection with this Type 2 surveillance operation and, except for the wrong entry as reported, found no irregularity. While agreeing generally to the recommendations stated in the investigation report, I considered that the long term remedial measure of using a memo for the return of surveillance devices should be implemented as soon as practicable. The LEA agreed and advised that it had implemented the use of the proposed memo form for the return of surveillance devices in ICSO operations since January 2013.

Report 3: Wrong description of rank of the approving officer

7.23 The LEA submitted a report in September 2012 on this incident which arose from the review of a prescribed authorization for Type 1 surveillance.

7.24 Section 8(3) of the Ordinance provides that an application for Type 1 surveillance may not be made to the panel judge unless the making of the application has been approved by a directorate officer of the department concerned. In an affidavit in support of an application for a prescribed authorization for Type 1 surveillance, an LEA wrongly

described the approving officer as 'A', which was a non-directorate rank, albeit he was in fact a directorate officer. The mistake was discovered by the reviewing officer during the review of the case in September 2012.

7.25 The LEA considered that the mis-description was a clerical mistake, which did not appear to have a material impact on the application concerned. It recommended that no further investigative action be taken but that the four officers (including the approving officer) who did not detect the mis-description during the application and/or review process be advised by a senior directorate officer on the need to exercise caution in scrutinizing application documents. Notwithstanding the mistake in the affidavit, there was no non-compliance with section 8(3) of the Ordinance as the approving officer was in fact a directorate officer at the time of approving the making of the application. I agreed that there was no evidence of improper conduct on the part of the concerned officers in this case and accepted the LEA's recommendations.

Report 4: An incident in which the information on the kind of device authorized by a Type 2 authorization was wrongly input into the DMS

7.26 The LEA submitted an incident report in November 2012 in which a surveillance device storekeeper selected a wrong checkbox in the DMS that incorrectly signified the approval for the issuance of listening devices in a Type 2 surveillance operation.

7.27 The investigation revealed that in a prescribed authorization, only optical devices were authorized for use in an operation. A total of eight optical devices were required to be withdrawn from the device store. The storekeeper mistakenly clicked the checkbox of 'Listening' in addition to that of 'Optical' when inputting

the type of devices data in the DMS. The storekeeper realised the mistake when he checked the print out on the list of devices issued. Upon receipt of the report of mistake, the storekeeper's supervisor directed the storekeeper to ensure that only optical devices be issued and to make a record in the remark column of the register on the mistake made. The LEA concluded that only optical devices were issued and there was no non-compliance to the conditions set out in the prescribed authorization. The mistake in the input might have been caused by carelessness on the part of the storekeeper and he should be held responsible for failing to input accurate information in accordance with the prescribed authorization. The officer had been reminded to be more vigilant in handling ICSO-related duties and follow proper procedures in the control of surveillance devices. A general reminder would be given to all device storekeepers to avoid recurrence in future.

7.28 I noted the report and LEA's findings. The storekeeper had promptly reported the incident to his supervisor when he discovered his mistake after checking the records of issue and admitted his fault. The mistake did not result in the issue of a listening device. Appropriate follow up actions had been taken by his supervisor. I considered that there was no evidence of improper conduct on the part of the officer concerned and agreed that the storekeeper should be reminded to be more vigilant in his duties.

Report 5: Technical problem with a recording device

7.29 At an inspection visit to an LEA in September 2012, in the course of examining the review folder of a prescribed authorization for a Type 1 surveillance operation, it was noted that the recording by a device deployed at the surveillance operation was unsuccessful due to a technical problem. The LEA was requested to conduct an investigation

and submit a report which should include the general procedure on the issue and return of all types of removable storage media.

7.30 The LEA's investigation report of November 2012 revealed that tests had been carried out to ascertain the reason for the technical problem of the recording device. While the actual cause was unknown, the LEA has since issued new procedural guidelines to ensure that devices are functioning properly before their deployment. It also proposed new procedures for the issue and return of all removable storage media.

7.31 I reviewed the case and found no irregularity, save that (as stated in the investigation report) the officer had used a wrong type of proforma when withdrawing the removable storage media. In this regard, I have asked the LEA to remind the officer concerned to be more vigilant in handling the withdrawal of removable storage media. While the proposed new procedures for the issue and return of removable storage media were a significant improvement on the past practice, I have suggested the LEA to consider using the computerised DMS to record these movements in the long term so as to reduce human error. I also advised the LEA to adopt the new procedures as soon as practicable. At the time of writing of this report the LEA is studying the technical issues involved.

Other reports

7.32 Of the remaining five reports submitted by the LEAs, these included four incidents of technical/system problems of the computerised systems and one case on incorrect use of a prescribed application form. These cases have been reviewed. All were relatively straight forward and nothing untoward was found. I was satisfied with the prompt action taken by the LEAs in the investigation

of the cases and proper follow up action taken to address the issues. For those relating to technical/system issues, appropriate follow up actions have been taken by the LEAs to fix the problems.

[This page is left blank.]

CHAPTER 8

RECOMMENDATIONS TO HEADS OF LAW ENFORCEMENT AGENCIES

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

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

(a) Better control of the issue and return of removable storage media

A serial number should be assigned to each of the removable storage media and a computerised DMS should be used to control the issue and return of the storage media.

(b) *The need to ensure that officers involved in the control mechanism for the movement of surveillance devices were properly trained, dedicated and focused*

In an endeavour to address the problems arising from careless mistakes, the LEA was urged to devote more time and effort to instil in officers implementing and supervising the control mechanism for the movement of surveillance devices the need for strict adherence to the ICSO procedures and that those officers who did not adhere to these objectives should not be deployed in this area of work.

(c) *Inclusion of the subject's relevant criminal records in application*

In applying for a prescribed authorization, the applicant should include in the application documents information on the subject's criminal records which were relevant to the offences being investigated.

CHAPTER 9

STATUTORY TABLES

9.1 In accordance with section 49(2), 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	506	0
	Average duration	29 days	-
(ii)	Number of authorizations renewed	655	Not applicable
	Average duration of renewals	31 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	41	Not applicable
(vi)	Number of applications for the issue of authorizations refused	1	0
(vii)	Number of applications for the renewal of authorizations refused	6	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	6	9	0
	Average duration	2 days	5 days	-
(ii)	Number of authorizations renewed	0	2	Not applicable
	Average duration of renewals	-	9 days	-
(iii)	Number of authorizations issued as a result of an oral application	0	2	0
	Average duration	-	10 days	-
(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 drugs	Cap. 134	Section 4, Dangerous Drugs Ordinance
Engaging in bookmaking	Cap. 148	Section 7, Gambling Ordinance
Managing a triad society/assisting in the management of a triad society	Cap. 151	Section 19(2), Societies 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
Theft	Cap. 210	Section 9, Theft Ordinance
Burglary	Cap. 210	Section 11, Theft Ordinance
Handling stolen property/goods	Cap. 210	Section 24, Theft Ordinance
Conspiracy to inflict grievous bodily harm/shooting with intent/wounding with intent	Cap. 212	Section 17, Offences Against the Person 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
Dealing with goods to which the Dutiable Commodities Ordinance applies	Cap. 109	Section 17(1), Dutiable Commodities Ordinance
Trafficking in dangerous drugs	Cap. 134	Section 4, Dangerous Drugs Ordinance
Engaging in bookmaking	Cap. 148	Section 7, Gambling Ordinance
Lending money at excessive interest rates	Cap. 163	Section 24, Money Lenders Ordinance
Criminal intimidation	Cap. 200	Section 24, 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
Burglary	Cap. 210	Section 11, Theft Ordinance
Taking conveyance without authority	Cap. 210	Section 14, Theft Ordinance
Blackmail	Cap. 210	Section 23, Theft Ordinance
Handling stolen property/goods	Cap. 210	Section 24, Theft Ordinance
Corrupt conduct to provide others with refreshments and entertainment at election	Cap. 554	Section 12, Elections (Corrupt and Illegal Conduct) 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 1]		
	Subject	**Non-subject**	**Total**
Interception	70	164	234

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 2]		
	Subject	**Non-subject**	**Total**
Surveillance	12	13	25

Note 1 Of the 234 persons arrested, ten were attributable to both interception and surveillance operations that had been carried out.

Note 2 Of the 25 persons arrested, ten 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 249.

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)]

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
<u>Section 41(1)</u> Reviews on compliance by departments and their officers with relevant requirements, as the Commissioner considers necessary			
(a) Regular reviews on weekly reports	212	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 212 weekly reports were submitted by the LEAs.
(b) Periodical inspection visits to LEAs	28	Interception & Surveillance	In addition to the checking of weekly reports, the Commissioner had paid 28 visits to LEAs during the report period. During the visits, the Commissioner conducted detailed checking on the application files of doubtful cases as identified from the weekly reports. Moreover, random inspection of other cases would also be made. Whenever he considered necessary, the Commissioner would seek clarification or explanation from LEAs directly. From the said inspection visits, a total of 631 applications and 239 related documents/matters had been checked. (See paragraphs 2.22, 3.21, 3.22 and 3.27 of this report.)

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
(c) LPP cases reviewed by the Commissioner	14	Inteception	<u>Outstanding LPP case in 2011</u> This case was brought forward from Annual Report 2011. The LEA had been asked to consider proposing actions to be taken against the officers concerned with the unsatisfactory handling of the LPP case. It replied that an officer would be verbally advised (disciplinary in nature) with a record on file. In addition, relevant officers working on ICSO-related duties were reminded of the requirement to submit an REP-11 report together with a discontinuance report in relation to the listening of Reported LPP Calls. The former Commissioner noted and did not raise objection to these actions. (See paragraph 5.11 of Chapter 5.)
		Interception	<u>LPP Case 1</u> The interception operation was not assessed to have a likelihood of obtaining LPP information at the grant of the prescribed authorization. As the interception progressed, after listening to part of a call, the listener formed the view that information subject to LPP had been obtained and she reported the matter to her supervisor who directed that the monitoring should be suspended. The LEA then submitted an REP-11 report to the panel judge and sought approval to resume the monitoring. After considering the REP-11 report, the panel judge allowed the prescribed authorization to continue with additional conditions imposed to guard against the risk of obtaining LPP information. On the same day that the monitoring of the operation resumed, the listener listened to part

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			of an intercepted call from another telephone number and formed the view that LPP information had been obtained and reported the matter up the chain of command. An REP-11 report and a discontinuance report were subsequently submitted to the panel judge who duly revoked the prescribed authorization. No recording of intercepted calls was listened to. Hence, no finding could be made as to the veracity of the content of the conversations in the Reported LPP Call as stated in the REP-11 reports. Similarly, no finding could be made as to whether the calls preceding the Reported LPP Call also had LPP information or likely LPP information or increased LPP likelihood that ought to have been reported to the panel judge, or whether there were any communications subject to LPP other than those reported. Subject to these qualifications, nothing untoward was found. (See paragraphs 5.7, 5.9 and 5.10 of Chapter 5.)
		Interception (12 reviews)	<u>The other 12 LPP cases</u> The review of these LPP cases was completed and nothing untoward was found, subject to the qualifications stated in LPP Case 1 above. (See paragraphs 5.8 – 5.10 of Chapter 5.)

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
(d) JM cases reviewed by the Commissioner	3	Interception (3 reviews)	<u>The three JM cases</u> The Commissioner conducted a review of these three JM cases. No irregularity was found. However, as he had not listened to the interception products, no findings could be made as to the veracity of the contents of the calls as stated in the REP-11 reports and whether apart from those calls, there were any other communications which might have contained JM in the interception products listened to by the LEA. (See paragraphs 5.13 – 5.17 of Chapter 5.)
(e) Incidents/ irregularities reviewed by the Commissioner	11	Interception	<u>Outstanding Case (ii) from 2011</u> This case was brought forward from Annual Report 2011. An LEA officer was found to have retained documents relating to interception operations conducted a few years earlier, which should have been destroyed within one month after the conclusion of the operations. The LEA concluded that the officer had breached the destruction policy stipulated in the departmental guidelines. No disciplinary action was recommended against the officer as the officer no longer served in the LEA. The Commissioner considered that this was not a case of 'non-compliance' because the LEA had issued guidelines to ensure that the destruction requirements under the ICSO and the COP were satisfied. The officer's act was in breach of these departmental guidelines. (See paragraphs 7.10 – 7.14 of Chapter 7.)

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
		Surveillance	Report 1 An officer responsible for vetting the device request form signed to confirm under the column 'Quantity issued' in the request form that one surveillance device was issued, although no device was issued that day. The LEA agreed that the literal interpretation of the term 'Quantity issued' meant the quantity of devices that had been issued and the practice adopted by the officer regarding the signing of device request form in the field 'Confirmed by:' under the column 'Quantity issued' before the actual issue of device(s) was due to his misinterpretation of the purpose and meaning of the term. The Commissioner considered that there was no evidence of deliberate disregard of the procedures for the control of surveillance devices on the part of the five officers involved in this case and had advised the LEA of his views on its proposed disciplinary actions against these officers. (See paragraphs 7.16 – 7.19 of Chapter 7.)
		Surveillance	Report 2 A Type 2 surveillance operation was discontinued but upon the return of surveillance devices used, it was erroneously represented in the device register that it would still continue as the device receiving officer was not informed of the discontinuance of the operation. There was a misunderstanding between the device receiving officer and the case officer about the time when the former should be notified of the discontinuance of an operation. As a long term measure, the LEA recommended to use a device return

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			form each time when devices were returned to avoid any ambiguity as to whether the operation would continue or not. The Commissioner considered that this measure should be implemented as soon as practicable. (See paragraphs 7.20 – 7.22 of Chapter 7.)
		Surveillance	<u>Report 3</u> In an affidavit in support of an application for a prescribed authorization for Type 1 surveillance, an LEA wrongly described the approving officer as 'A', which was a non-directorate rank, albeit he was in fact a directorate officer. The LEA recommended that no further investigative action be taken but that the four officers (including the approving officer) who did not detect the mis-description during the application and/or review process be advised by a senior directorate officer on the need to exercise caution in scrutinizing application documents. The Commissioner agreed that there was no evidence of improper conduct on the part of the concerned officers in this case and accepted the LEA's recommendations. (See paragraphs 7.23 – 7.25 of Chapter 7.)
		Surveillance	<u>Report 4</u> A Type 2 authorization authorized only optical devices for use in an operation, but a surveillance device storekeeper mistakenly clicked the checkbox of 'Listening' in addition to that of 'Optical' when inputting the type of devices in the DMS. The mistake did not result in the issue of a

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			listening device. (See paragraphs 7.26 – 7.28 of Chapter 7.) Surveillance <u>Report 5</u> The recording by a device deployed at a surveillance operation was unsuccessful due to a technical problem. The LEA's investigation report revealed that, while the actual cause was unknown, the LEA has since issued new procedural guidelines to ensure that devices are functioning properly before their deployment. It also proposed new procedures for the issue and return of all removable storage media. The Commissioner has reviewed the case and found no irregularity, save that an officer had used a wrong type of proforma when withdrawing the removable storage media. He has asked the LEA to remind the officer to be more vigilant in handling the withdrawal of removable storage media. He suggested the LEA to consider using the computerised DMS to record the movements of removable storage media in the long term so as to reduce human error. He also advised the LEA to adopt the new procedures as soon as practicable. (See paragraphs 7.29 – 7.31 of Chapter 7.) Interception & Surveillance (5 reviews) <u>Other reports</u> The Commissioner has reviewed all these cases which were relatively straight forward and found nothing untoward. He was satisfied with the prompt action taken by the LEAs in the investigation of the cases and proper follow up action taken to

Number of reviews conducted under section 41(1)		Interception/ Surveillance	Summary of reviews
			address the issues. For those relating to technical/system issues, appropriate follow up actions have been taken by the LEAs to fix the problems. (See paragraph 7.32 of Chapter 7.)

Number of reviews conducted under section 41(2)	Interception/ Surveillance	Summary of reviews
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		
(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.

Number of reviews conducted under section 41(2)		Interception/ Surveillance	Summary of reviews
(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	1	Interception	<u>Outstanding Case (i) from 2011</u> This case was brought forward from Annual Report 2011, involving a breach of the revised additional conditions imposed by the panel judge in the prescribed authorization for interception to guard against the risk of obtaining LPP information. The LEA indicated that a conclusion could not be drawn that its management and senior officers concerned should have appreciated the risk of non-compliance with the revised additional conditions, which was agreed by the former Commissioner. While the case had not been handled by the LEA officers satisfactorily, there was no evidence of ulterior motive or ill will on the part of the LEA management or any of the officers concerned. The Commissioner had no objection to the proposed verbal warning for each of the three officers concerned. (See paragraphs 7.6 – 7.9 of Chapter 7.)

Table 6

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

Number of cases of irregularities or errors identified in the reviews under section 41(1)		Interception/ Surveillance	Broad nature of irregularities or errors identified
Section 41(1)			
(a) Reviews of LPP cases pursuant to paragraph 121 of the Code of Practice	1	Interception	<u>Outstanding LPP case in 2011</u> Unsatisfactory handling of the case by the LEA. The normal practice of submitting an REP-11 report stating whether there were any 'other calls' between the telephone numbers involved in the LPP call was not followed. There was also a dispute as to what material the LEA had examined as the basis for stating that there were only eight such 'other calls' but in fact there were 26 'other calls'. (For details, see item (c) under section 41(1) in Table 5 and Chapter 5.)
(b) Other reviews	11	Interception	<u>Outstanding Case (ii) from 2011</u> Retention by an LEA officer of documents relating to interception operations, which was in breach of departmental guidelines.
		Surveillance	<u>Report 1</u> Misinterpretation of a term used in the device request form.
		Surveillance	<u>Report 2</u> Erroneous representation in the device register that a surveillance operation would still continue upon the return of surveillance devices despite the operation was discontinued.

Number of cases of irregularities or errors identified in the reviews under section 41(1)		Interception/ Surveillance	Broad nature of irregularities or errors identified
		Surveillance	<u>Report 3</u> Wrong description of rank of the approving officer in an affidavit in support of an application for a prescribed authorization for Type 1 surveillance.
		Surveillance	<u>Report 4</u> Wrong input of information on the kind of device authorized by a prescribed authorization for Type 2 surveillance into the DMS.
		Surveillance	<u>Report 5</u> Technical problem with a recording device during covert surveillance operation.
		Interception & Surveillance (5 cases)	<u>Other reports</u> These included four incidents of technical/system problems of the computerised systems and one case on incorrect use of a prescribed application form. (For details, see item (e) under section 41(1) in Table 5 and Chapter 7.)

Number of cases of irregularities or errors identified in the reviews under section 41(2)		Interception/ Surveillance	Broad nature of irregularities or errors identified
Section 41(2)			
(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	893	Interception	<u>Outstanding Case (i) from 2011</u> 893 instances of non-compliance with the revised additional conditions imposed by panel judges in prescribed authorizations for interception. (See item (c) under section 41(2) in Table 5 and Chapter 7.)

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
18	4	1	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 3	11	4	1	6

Note 3 Of the 11 notices, five were issued during the reporting period and six 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 Code of Practice [section 51]	Nil	Not applicable	Not applicable
Recommendations to departments for better carrying out the objects of the Ordinance or the provisions of the Code of Practice [section 52]	3	Interception & Surveillance	(a) *Better control of the issue and return of removable storage media* (i) assigning a serial number to each of the removable storage media; and (ii) using computerised DMS to better control the issue and return of the removable storage media. (b) *The need to ensure that officers involved in the control mechanism for the movement of surveillance devices were properly trained, dedicated and focused* (i) devoting more time and effort to instil in LEA

Recommendations made by the Commissioner		Interception/ Surveillance	Broad nature of recommendations
			officers implementing and supervising the control mechanism for the movement of surveillance devices the need for strict adherence to the ICSO procedures; and (ii) not deploying officers who did not adhere to these objectives in this area of work. (c) *Inclusion of the subject's relevant criminal records in application* Including subject's criminal records which were relevant to the offences being investigated in the application for a prescribed authorization. (See paragraph 8.2 of Chapter 8.)

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	1
Surveillance	0

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	A listener listened to a call made to a prohibited number set out in the additional conditions imposed by the panel judge. (See paragraphs 7.8 – 7.13 of Chapter 7 of Annual Report 2011.)	Verbal warning
<u>Case 2</u> Surveillance	(i) An officer-in-charge of the operation failed to ensure the inclusion of correct information in the affirmation in support of the application.	Written warning
	(ii) The applicant of the application for authorization for covert surveillance, who was also the supervisor of the officer mentioned in (i) above, failed to ensure the inclusion of correct information in the affirmation in support of the application.	Written warning
	(iii) The reviewing officer of the covert surveillance operation failed to notice the incorrect statement in the affirmation in support of the application during the review process. (See paragraphs 7.125 – 7.138 of Chapter 7 of Annual Report 2011.)	Verbal warning

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<u>Case 3</u> Surveillance	A device issuing officer deliberately entered false information into device register to pretend that the devices concerned were issued for an operation authorized under a prescribed authorization. (See paragraphs 7.139 – 7.158 of Chapter 7 of Annual Report 2011.)	Reprimand
<u>Case 4</u> Interception	(i) An officer tasked with drafting an REP-11 report on heightened likelihood of obtaining LPP information omitted to mention a related call in the report. (ii) The reporting officer of the REP-11 report above failed to detect the omission. (See paragraphs 5.69 – 5.83 of Chapter 5 of Annual Report 2011.)	Verbal advice Verbal advice

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
<u>Case 5</u> Interception	(i) An officer tasked with drafting an REP-11 report on heightened likelihood of obtaining LPP information accessed a call when monitoring was supposed to be put on hold and failed to mention this access in the REP-11 report. (ii) The reporting officer of the REP-11 report, who was also the supervisor of the officer mentioned in (i) above, failed to ensure that the access right to the interception operation had been properly removed for suspending the monitoring and that the REP-11 report submitted to the panel judge contained all necessary and material information. (See paragraphs 7.50 – 7.92 of Chapter 7 of Annual Report 2011.)	Verbal warning Verbal advice

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
Case 6 Interception	(i) An officer responsible for investigating the crime provided a wrong telephone number to the officer mentioned in (ii) below and failed to detect the error on a number of occasions, leading to unauthorized interception of a wrong facility.	Written warning
	(ii) The officer-in-charge of the ICSO registry who headed the dedicated application team failed to discharge her supervisory responsibility and detect the error on a number of occasions.	Written warning
	(iii) The applicant of the application for authorization for interception, who was also the supervisor of the officer mentioned in (ii) above, failed to discharge his supervisory responsibility and personally check the correctness of the telephone number before signing off the application document.	Written warning
	(iv) The assistant processing officer of the dedicated application team failed to detect the discrepancy between the telephone number shown on the draft application documents and the number shown on the verification form.	Written warning
	(v) The processing officer of the dedicated application team failed to detect the discrepancy between the telephone number shown on the draft application documents and the number shown on the verification form. (See paragraphs 7.159 – 7.188 of Chapter 7 of Annual Report 2011.)	Written warning of dismissal

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
Case 7 Interception	(i) An officer made a less than accurate assessment as to whether a suspected LPP call she had listened to contained LPP information. (ii) The supervisor of the officer mentioned in (i) above, adopted a wrong approach towards dealing with a suspected LPP call. It was wrong for him to task the officer with listening to the call so as to clarify if the call really contained LPP information. He also made a less than accurate assessment as to whether the call contained LPP information. (See paragraphs 5.18 – 5.44 of Chapter 5 of Annual Report 2011.)	Verbal advice Verbal advice

Case number and nature of operation	Brief facts of case	Broad nature of the disciplinary action
Case 8 Interception	(i) A junior listener inadvertently listened to a call which, in accordance with the LPP additional conditions imposed on the prescribed authorization concerned, should be listened to only by officers of higher rank. (ii) A junior listener inadvertently listened to a call which, in accordance with the LPP additional conditions imposed on the prescribed authorization concerned, should be listened to only by officers of higher rank. (iii) A junior listener inadvertently listened to five calls which, in accordance with the LPP additional conditions imposed on the prescribed authorization concerned, should be listened to only by officers of higher rank. (See paragraphs 7.93 – 7.114 of Chapter 7 of Annual Report 2011.)	Verbal advice Verbal advice Verbal warning

9.2 In accordance with section 49(2)(e), 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 10.

[This page is left blank.]

CHAPTER 10

REVIEW OF COMPLIANCE BY LAW ENFORCEMENT AGENCIES

Overall compliance

10.1 As set out in section 40 of the Ordinance, the functions of the Commissioner are to oversee the compliance by departments and their officers with the relevant requirements and to conduct reviews, etc. It is also 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.

10.2 On the whole, I was satisfied with the overall performance of the LEAs and their officers in their compliance with the relevant requirements of the ICSO in 2012.

Preparation of applications

10.3 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.

10.4 During the report period, most of the applications for interception made by the LEAs were granted with only a very small number of applications being refused by the panel judges (seven out of 1,168 applications). In respect of applications for Type 1 or Type 2 surveillance, all were granted. It well demonstrates that the LEAs have adopted a cautious approach in applying for prescribed authorizations, their preparation of the applications for interception and covert surveillance operations was of a good standard and they did observe the necessity and proportionality principles.

Reviews by the Commissioner

10.5 There were different ways by which compliance with the requirements of the Ordinance in respect of interception and covert surveillance by the LEAs was reviewed as set out in paragraph 2.16 of Chapter 2 and paragraph 3.18 of Chapter 3. These included checking of the weekly reports submitted by the LEAs and the PJO, periodical examination of the contents of the LEA files and documents during inspection 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, there would be checking of the records kept by the surveillance device recording system of the LEAs.

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

In respect of covert surveillance, while there were some areas for improvement, most of the cases checked during inspection visits were found to be in order. Generally, there was no sign of abuse of surveillance devices for any unauthorized purposes during the report period.

Handling of LPP and JM cases

10.7 Paragraph 121 of the COP obliges the concerned LEA to notify the Commissioner of cases that are likely to involve LPP information or JM. I am also timeously alerted to cases involving or possibly involving LPP and JM through the examination of the weekly reports submitted by the LEAs, with sanitized copies of the relevant REP-11 reports reporting on any material change of circumstances after the issue of a prescribed authorization including changed LPP and JM risks.

10.8 The LEAs did recognise the importance of protecting information which might be subject to LPP/JM. They continued to adopt a very cautious approach in handling these cases. In the report period, no irregularities were found.

Reports of non-compliance/irregularities

10.9 Under section 54 of the Ordinance, the heads of LEAs are to submit reports to the Commissioner if they consider that there may have been any case of failure by the department or any of its officers to comply with any relevant requirement of the Ordinance. They are also required to report to the Commissioner cases of irregularity or even simply incidents. Hence, I am able to have all cases of possible

non-compliance brought to my attention for examination and review without any delay.

10.10 In 2012, all the reports of irregularities/incidents made to the Commissioner were submitted not under section 54 of the Ordinance i.e. they are not non-compliance cases. In the report period, save for Case B which involved a false report of a storekeeper mentioned in Chapter 4, neither myself nor my predecessor have made findings that any of the other cases of irregularity/incidents was due to deliberate disregard of the statutory provisions, the COP or the control of surveillance devices. While the mistakes or errors are to be regretted, it is obvious that the incidents were the consequences of inadvertent or careless mistakes or occasionally unfamiliarity on the part of officers with the rules and procedures of the ICSO scheme.

A more focused and responsible mind set

10.11 While the overall compliance was satisfactory, there was still room for improvement for all LEA officers in carrying out their duties. One of the matters of concern to my predecessor and a concern which I share is that some of the officers of the LEAs handling ICSO-related matters appeared to approach the discharge of their duties in such a way as indicates that they do not appreciate the significance of the need for strict regulation of ICSO-related matters and strict adherence to the ICSO scheme. I believe that the LEAs need to concentrate on developing a more focused and responsible mind set in officers at all levels responsible for the operation of the ICSO scheme.

10.12 During the period of my tenure as Commissioner there was one case which caused me the most concern which I have reported earlier (Case B in Chapter 4). There was an incident in March 2012

where a device storekeeper failed to record the return of certain devices upon the conclusion of a non-ICSO operation. Realising his mistake rather than report the true situation, he fabricated an account to the effect that there had been a power failure at the time and this was the reason that the return of the devices could not be recorded. The officer's conduct was dishonest. What was of equal, if not greater, concern was the failure of that LEA upon becoming aware of the confession of the officer to notify the Commissioner immediately. That confession was made in late March 2012 and yet the LEA wrote to my predecessor 12 days later and said inter alia that *'It would appear that the initial version as given by the device store keeper … may not be entirely true'.* I have advised the head of the LEA concerned that this was unquestionably a misleading assertion. There must be prompt, full and frank disclosure to the Commissioner at all times. This did not happen on this occasion and should not happen again.

Positive response

10.13 Whilst I have observed that there have been cases of carelessness and at times insufficient focus, I have been encouraged in the course of the report period by the positive response from the LEAs to initiatives I have made to address problem areas. My predecessor actively encouraged all LEAs to pursue the introduction of computer based processes designed and intended to minimize manual input into the system and thus reduce unnecessary human error. I have likewise stressed the importance of this. I am encouraged by the positive response of the LEAs to this and would hope to be in a position in my next report to advise fully on the progress of those initiatives. I believe that the LEAs are fully alert to the benefits that would flow to all, not least of all the officers administering the ICSO scheme if the possibility of human error can be significantly reduced or eliminated.

Necessary deterrence

10.14 It is clear that the report of most cases of non-compliance or irregularity in the past was done by the LEAs of their own accord. Without such voluntary compliance by the LEAs, it would be difficult, if not impossible, for the Commissioner and his staff to discover or unearth any contravention by the LEAs. A necessary deterrence against any contravention or abuse of the Ordinance or prescribed authorizations or its concealment by the LEAs and their officers can be achieved by the recommendation made in past reports on providing for the Commissioner and his designated staff to have the power to check the audio interception products or examination of surveillance products. I believe this is entirely appropriate and would be the ultimate deterrence for those who would be minded to breach the requirements under the ICSO scheme.

CHAPTER 11

ACKNOWLEDGEMENT AND WAY FORWARD

Acknowledgement

11.1 My task as the Commissioner could not be carried out satisfactorily without all the help and co-operation of the panel judges, the Security Bureau, the LEAs as well as the CSPs. I would like to express my gratitude to each and every one of them and look forward to their continued support in the course of my term of office.

Way forward

11.2 The Administration is undertaking a comprehensive review of the Ordinance with the aim of further enhancing the operation of the ICSO regime. This review is being conducted with earlier recommendations made by my predecessor in mind. While I would welcome any improvements proposed for the ICSO scheme, I would wish to point out that the most important recommendation identified by my predecessor is to give the Commissioner and the staff as designated by him the express legal power necessary for listening to, viewing and monitoring the products from interception and covert surveillance as the Commissioner chooses because he considered that this would be the primary tool to expose any malpractices of the LEAs and their officers and would act as a forceful deterrent against such malpractices and their concealment. These are sentiments which I unreservedly endorse. It suffices to say at this stage that this matter is under active consideration and I would hope to be in a better position to advise more fully in my next report.