

香港特別行政區政府  
保安局



LC Paper No. CB(2)443/15-16(01)

The Government of the  
Hong Kong Special Administrative Region  
Security Bureau

香港添馬添美道 2 號

2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.: SBCR 14/2/3231/94 Pt. 26

來函檔號 Your Ref.:

電話號碼 TEL. NO.: 2810 2632

傳真號碼 FAX. NO.: 2877 0636

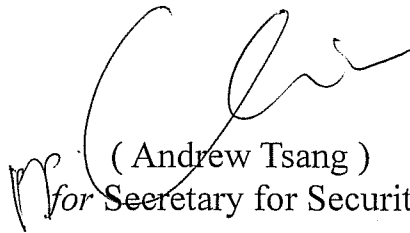
11 December 2015

Miss Betty Ma  
Legislative Council Secretariat  
Legislative Council Complex  
1 Legislative Council Road  
Central, Hong Kong

Dear Miss Ma,

We refer to the meetings of Bills Committee on Interception of Communications and Surveillance (Amendment) Bill 2015 on 9 and 16 November 2015, and Members' proposed Committee Stage Amendments (CSAs). A paper setting out the further CSAs proposed by the Government, and the Government's response to Members' proposed CSAs and other issues raised at the Bills Committee meetings on 9 and 16 November 2015 is at Annex.

Yours sincerely,



( Andrew Tsang )  
for Secretary for Security

Encl (21 pages)

c.c.

Department of Justice

(Attn: Mr Godfrey Kan, Senior Assistant Solicitor General  
Ms Monica Law, Senior Assistant Law Draftsman)

**Interception of Communications  
and Surveillance (Amendment) Bill 2015  
("the Bill")**

**Further Committee Stage Amendments ("CSAs")  
Proposed by the Government, and  
Response to Members' Proposed CSAs and Issues Raised  
at the Bills Committee's Meetings on 9 and 16 November 2015**

**(a) Further CSAs Proposed by the Government**

Further to the CSAs proposed by the Government viz LC Paper No. CB(2)214/15-16(01) and having regard to the concerns raised by the Bills Committee, we propose further CSAs to extend the checking power of the Commissioner on Interception of Communications and Surveillance ("the Commissioner") to cover any protected products that are currently subject to immediate destruction under sections 23(3)(a), 24(3)(b), 26(3)(b)(i) and 27(3)(b) of the Interception of Communications and Surveillance Ordinance ("ICSO") (Cap 589).

2. The CSAs, marked-up version at **Appendix I**, are in line with the proposed amendments to section 59(1)(c) of the ICSO in clause 19 of the Bill which aims to provide for the destruction of protected products that have been provided to the Commissioner, and the proposed amendments to section 53(1)(a) in clause 13 of the Bill which aims to empower the Commissioner to require any public officer or any other person to provide any protected product (whether or not it contains any information that is or may be subject to legal professional privilege) in his possession or control to the Commissioner. The purpose of these CSAs is to give full effect to the recommendations of the first Commissioner that (i) the Commissioner should be given the express power and unfettered discretion to examine protected products of his choice, which would pose as a useful and strong deterrent against the law enforcement agencies ("LEAs") doing anything unauthorised or concealing any unauthorised acts, and that (ii) the requirement to destroy protected products should be made subject to the Commissioner's power to examine them. These recommendations are endorsed by the second Commissioner and agreed by the Administration.

3. Section 23(3)(a) of the ICSO provides that if an application for confirmation of an emergency authorization is not made within 48 hours beginning with the time when the emergency authorization is issued, the head of an LEA shall cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned. There is also a similar provision in section 26(3)(b)(i) in respect of a failure to apply for confirmation of a prescribed authorization issued, or a renewal granted, upon an oral application. Where an LEA has made an application for confirmation in compliance with section 23(1) or 26(1) but the relevant authority refuses to confirm the authorization or renewal in question, the relevant authority has a discretionary power to make an order under section 24(3)(b) or 27(3)(b) (as the case may be) for the immediate destruction of any information obtained by carrying out the operation concerned.

4. As explained in LC Paper No. CB(2)214/15-16(01), the destruction arrangements under sections 23(3)(a), 24(3)(b), 26(3)(b)(i) and 27(3)(b) are related to either serious non-compliance or a failure to meet the stringent threshold for the issue of a prescribed authorization and hence, immediate destruction of the information obtained is an appropriate remedy. These provisions also recognise the importance of protecting the privacy of the affected persons and deterring the LEAs from breaching the relevant requirements.

5. In line with the proposals in clauses 13 and 19 of the Bill and in order to give full effect to the first Commissioner's recommendations, we propose to introduce CSAs so that the Commissioner will be able to gain access to **all** protected products, including those referred to sections 23(3)(a), 24(3)(b), 26(3)(b)(i) and 27(3)(b) before they may be destroyed by the LEAs, thus striking a proper balance between privacy protection, deterrent against LEAs' abuse of power and effective oversight by the Commissioner of LEAs' compliance with the relevant requirements.

#### **(b) Response to Members' CSAs**

6. Our response to the proposed CSAs by Hon Dennis KWOK and Hon James TO is at **Appendix II**.

**(c) Other Issues Raised in the Meetings on 9 and 16 November 2015**

7. Our response to other issues raised at the Bills Committee meetings on 9 and 16 November 2015 is at **Appendix III**.

**Security Bureau  
December 2015**

## Appendix I

*Amendments proposed in the Bill in bold italics*

Government's proposed CSAs in track mode

Chapter:	589	Title:	<b>INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE ORDINANCE</b>
Section:	59	Heading:	<b>Safeguards for protected products</b>

(1) Where any protected product has been obtained pursuant to any prescribed authorization issued or renewed under this Ordinance on an application by any officer of a department, the head of the department shall make arrangements to ensure—

- (a) that the following are limited to the minimum that is necessary for the relevant purpose of the prescribed authorization—
  - (i) the extent to which the protected product is disclosed;
  - (ii) the number of persons to whom any of the protected product is disclosed;
  - (iii) the extent to which the protected product is copied; and
  - (iv) the number of copies made of any of the protected product;
- (b) that all practicable steps are taken to ensure that the protected product is protected against unauthorized or accidental access, processing, erasure or other use; and
- ~~(c) that the protected product is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization.~~
- (c) that, except as otherwise provided in subsection (1A), the protected product—
  - (i) *is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization, unless it is to be or has been provided to the Commissioner in compliance with a requirement imposed under section 53(1)(a) before it is so destroyed; or*
  - (ii) *if it has been provided to the Commissioner in compliance with a requirement imposed under section 53(1)(a), is, after it is no longer required by the Commissioner, destroyed as soon as its retention is not necessary—*
    - (A) *for the relevant purpose of the prescribed authorization; and*
    - (B) *if further requirements are imposed by the Commissioner under section 53(1)(a), for the purpose of enabling compliance with the requirements.*

(1A) Subsection (1B) applies if the protected product consists of information described in section 23(3)(a), 24(3)(b)(i) or (ii), 26(3)(b)(i) or 27(3)(b)(i) or (ii).

(1B) Despite section 23(3)(a) or 26(3)(b)(i) or any requirement in an order made under section 24(3)(b) or 27(3)(b), the head of the department concerned—

(a) must immediately notify the Commissioner of the case;

(b) must make arrangements to ensure that the information is retained; and

(c) must—

(i) if the Commissioner notifies the head of the department that the Commissioner will not require the provision of the information under section 53(1)(a), cause the immediate destruction of the information;  
or

(ii) if the Commissioner requires the provision of the information under section 53(1)(a)—

(A) provide the information as required; and

(B) cause the immediate destruction of the information when it is no longer required by the Commissioner.

(2) Where any protected product described in subsection (1) contains any information that is subject to legal professional privilege, subsection (1)(c) is to be construed as also requiring the head of the department concerned to make arrangements to ensure that any part of the protected product that contains the information—

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

(3) For the purposes of this section, something is necessary for the relevant purpose of a prescribed authorization—

- (a) in the case of subsection (1)(a), if—
  - (i) it continues to be, or is likely to become, necessary for the relevant purpose; or
  - (ii) except in the case of a prescribed authorization for a telecommunications interception, it is necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted; or
- (b) in the case of subsection (1)(c)—
  - (i) when it continues to be, or is likely to become, necessary for the relevant purpose; or
  - (ii) except in the case of a prescribed authorization for a telecommunications interception, at any time before the expiration of 1 year after it ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted.

《條例草案》擬議的修訂以粗斜體標記

政府建議修正案以標明修訂方式標記

章：	589	標題：	《截取通訊及監察條例》
條：	59	條文標題：	對受保護成果的保障

(1) 凡訂明授權因應部門的任何人員提出的申請而根據本條例發出或續期，而任何受保護成果依據該授權而被取得，該部門的首長須作出安排，以確保—

- (a) 以下事宜被限制於對該訂明授權的有關目的屬必要的最小限度—
  - (i) 受保護成果的披露範圍；
  - (ii) 屬受保護成果披露對象的人的數目；
  - (iii) 受保護成果被複製的程度；及
  - (iv) 以任何受保護成果製成的文本的數目；
- (b) 已採取所有切實可行步驟，以確保受保護成果已獲保護而不會在未經授權下或在意外的情況下被取用、處理、刪除或用作其他用途；及
- ~~(c) 在保留受保護成果並非對訂明授權的有關目的屬必要時，盡快銷毀該等成果。~~
- (c) 除第(1A)款另有規定外，受保護成果按照以下規定銷毀—
  - (i) 在保留該成果對該訂明授權的有關目的並非屬必要時，盡快予以銷毀，但如在如此銷毀之前，該成果將會或已經為遵從根據第53(1)(a)條施加的要求而向專員提供，則屬例外；或；
  - (ii) 如已經為遵從根據第53(1)(a)條施加的要求而向專員提供該成果，於專員不再需要該成果後，在保留該成果—
    - (A) 對該訂明授權的有關目的；及
    - (B) (如專員根據第 53(1)(a)條施加進一步要求)對使該等要求得以遵從，並非屬必要時，盡快予以銷毀。

(1A) 如受保護成果屬第23(3)(a)、24(3)(b)(i)或(ii)、26(3)(b)(i)或27(3)(b)(i)或(ii)條所描述的資料，則第(1B)款適用。

(1B) 儘管有第23(3)(a)或26(3)(b)(i)條的規定，亦儘管根據第24(3)(b)或27(3)(b)條作出的命令有任何規定，有關部門的首長 —

- (a) 須即時將有關個案通知專員；
- (b) 須作出安排，以確保有關資料獲得保留；及
- (c) 須按以下規定行事 —
  - (i) 如專員通知該部門的首長，指專員不會根據第53(1)(a)條要求提供該等資料，則須安排將該等資料即時銷毀；或
  - (ii) 如專員根據第53(1)(a)條要求提供該等資料，則須 —
    - (A) 按要求提供該等資料；及
    - (B) 安排於專員不再需要該等資料時，將該等資料即時銷毀。

(2) 凡第(1)款所描述的任何受保護成果包含享有法律專業保密權的任何資料，則第(1)(c)款須解釋為亦規定有關部門的首長作出安排，以確保受保護成果中包含該等資料的部分—

- (a) (就對郵件截取或秘密監察的訂明授權而言)在自保留該部分對在任何法院進行的待決民事或刑事法律程序，或對相當可能會在任何法院提起的民事或刑事法律程序不再屬必要時起計的1年期間屆滿之前被銷毀；或
- (b) (就對電訊截取的訂明授權而言)於合理地切實可行範圍內盡快被銷毀。

(3) 就本條而言，在以下情況下，某事宜即屬對訂明授權的有關目的屬必要—

- (a) 在第(1)(a)款所指的情況下—
  - (i) 該事宜繼續是或相當可能變為是對該有關目的屬必要的；或
  - (ii) (除對電訊截取的訂明授權外)就於任何法院進行的待決民事或刑事法律程序而言，或就相當可能會在任何法院提起的民事或刑事法律程序而言，該事宜屬必要；或
- (b) 在第(1)(c)款所指的情況下—
  - (i) 該事宜繼續是或相當可能變為是對該有關目的屬必要的；或
  - (ii) (除對電訊截取的訂明授權外)就於任何法院進行的待決民事或刑事法律程序而言，或就相當可能會在任何法院提起的民事或刑事法律程序而言，在自該事宜對該等程序不再屬必要時起計的1年期間屆滿之前。



Government's Response to Members' CSAs

(a) Hon Dennis Kwok's CSAs

Clause 4 – New Section 3(3)

Hon Dennis Kwok proposes to move an amendment to clause 4 of the Bill. The proposed amendment seeks to declare “for the avoidance of doubt” that a prescribed authorization must not be for the purpose of (a) an act to obtain the content of communication stored in or by the system, or (b) an act to obtain data (other than that already in the public domain) held or obtained by a telecommunications service operator; and to require a public officer intending to conduct such an act to apply for a seizure order from a magistrate or the Court of First Instance pursuant to section 103 (Seizure of things intended for use in commission of indictable offence) of the Criminal Procedure Ordinance (Cap. 221).

2. The ICSO regulates the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers. Under the ICSO, interception of communications is prohibited unless it is carried out pursuant to a prescribed authorization (defined in the ICSO to mean a judge’s authorization, an executive authorization or an emergency authorization).

3. As defined in section 2(1) of the ICSO, “**interception**”, in relation to any communication, means the carrying out of any intercepting act in respect of that communication; or when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of any communication; and “**intercepting act**”, in relation to any communication, means the inspection of some or all of the contents of the communication, in the course of its transmission by a postal service or by a telecommunications system, by a person other than its sender or intended recipient.

4. Under the ICSO, if a communication is transmitted by a telecommunications system<sup>1</sup>, and an LEA intercepts the communication in the course of its transmission, then the interception will be regarded as an

---

<sup>1</sup> The term “telecommunications system” in the ICSO has the same meaning as that given to the term in section 2(1) of the Telecommunications Ordinance (Cap 106), i.e. “any telecommunications installation, or series of installations, for the carrying of communication by means of guided or unguided electromagnetic energy or both”.

“intercepting act”. The LEA must obtain an authorization from a panel judge before it may conduct such interception, and such interception operations are subject to the oversight of the Commissioner.

5. As can be seen in the Legislative Council Brief on the Bill dated 4 February 2015 and the Explanatory Memorandum of the Bill, the object of the Bill is to amend the ICSO to implement the recommendations made by the first Commissioner. The subject matter of the Bill, as can be seen in the long title and its substantive provisions, is to amend the ICSO to provide for the revocation of device retrieval warrants, partial revocation of prescribed authorizations and additional grounds for revoking prescribed authorizations; to allow conditions in prescribed authorizations to be varied; to clarify the meanings of certain expressions; to treat certain protected products obtained after the prescribed authorizations concerned are revoked to be properly obtained; to require a department head to report a failure to comply with a relevant requirement that is not due to the department’s fault; to enable the Commissioner to require the provision of protected products and to delegate the power to examine them; to make minor textual amendments; and to provide for related matters.

6. The amendment proposed by Hon Dennis KWOK relates to applications for a court order under section 103 of the Criminal Procedure Ordinance (Cap. 221) to obtain information or data held by a telecommunications service provider or any other person. The order referred to in the proposed section 3(3) of the Ordinance authorizes an operation which will become overt upon granting of the order by a magistrate or the Court of First Instance, and is by nature different from the covert operations regulated by the ICSO. The proposed amendment is not amongst any of the first Commissioner’s recommendations which the Bill seeks to implement.

(b) Hon James TO's CSAs

Clause 3 - Section 2(5)(b)

7. Hon James TO's proposed amendment seeks to amend clause 3 of the Bill.

8. The ICSO regulates the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers. **Interception** of a communication by a public officer is prohibited unless it is carried out pursuant to a prescribed authorization (defined in the ICSO to mean a judge's authorization, an executive authorization or an emergency authorization). Under the ICSO, "interception", in relation to any communication, means "the carrying out of any **intercepting act** in respect of that communication"; and an "intercepting act", in relation to any communication, means "the inspection of some or all of the contents of the communication, **in the course of its transmission** by a postal service or by a telecommunications system, by a person other than its sender or intended recipient" (**emphasis added**). Hence, the inspection of the contents of any communication that is not in the course of its transmission does not constitute an "intercepting act", and the inspection of such contents is not regulated by the ICSO.

9. Under the existing section 2(5)(b), "a communication transmitted by a telecommunications system is **not** regarded as being **in the course of the transmission** if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication". Hon James TO's proposed amendment seeks to reverse the definition of a communication transmitted by a telecommunication system "**in the course of its transmission**" by making it cover any communication which has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication. This proposed amendment fundamentally changes the scope of the ICSO and is out of line with the policy intent as articulated in the ICSO.

10. Apart from the above, seen against the Legislative Council Brief and the Explanatory Memorandum of the Bill as elaborated in paragraph 5, and the objective of clause 3 of the Bill which is to "amend the definitions of device retrieval warrant, emergency authorization, executive authorization and judge's authorization in section 2(1) of the [ICSO]", Hon James TO's proposed

amendment is not amongst the first Commissioner's recommendations and does not appear to relate to the substance or subject matter of clause 3 or the Bill.

### **Clause 19 - Section 59**

11. Hon James TO's proposed amendment seeks to amend clause 19 of the Bill to introduce criminal sanctions for destroying a protected product when it is required to be provided to the Commissioner under section 59(1)(c) of the ICSO as amended by clause 19 (hereinafter "the amended section 59(1)(c)").

12. Under the existing section 59(1)(c), a protected product is to be destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization. The first Commissioner recommended that the requirement to destroy protected products under section 59 should be made subject to the Commissioner's requirement to examine the protected products. In this regard, clause 19 seeks to amend section 59(1)(c) to provide for the destruction of protected products that have been provided to the Commissioner in compliance with a requirement imposed by the Commissioner under section 53(1)(a). Under the amended section 59(1)(c), a protected product should be destroyed once its retention is not necessary for the relevant purpose of the prescribed authorization unless the Commissioner imposes a requirement under section 53(1)(a) as amended by clause 13 that the protected product be provided to him for the purpose of performing his functions. Hon James TO's proposed amendment seeks to create an offence of destroying a protected product when it is required to be provided to the Commissioner under the amended section 59(1)(c) which is punishable with a maximum penalty of 2 years' imprisonment.

13. The ICSO does not provide for any criminal sanctions. It is the Administration's position that the question on whether criminal sanctions should be introduced under the ICSO has to be considered holistically alongside with the relevant bureau's deliberation on the Law Reform Commission ("LRC")'s recommendations regarding the interception or covert surveillance conducted by persons who are not public officers. In this regard, the relevant bureau has studied the reports by the LRC on "Regulating the Interception of Communications" and "The Regulation of Covert Surveillance". Due to mixed responses and divergent views from different sectors of the community, the relevant bureau is still considering the way forward. Pending the outcome of the bureau's deliberation, we have no plan to consider introducing criminal offences under the ICSO.

14. Currently, LEA officers are already under a statutory duty to comply with the relevant requirements, and their compliance with the ICSO and the

CoP is subject to very stringent oversight by the Commissioner. Officers in default are subject to disciplinary actions. In very serious cases with wilful intent, an officer may even be prosecuted for the common law offence of misconduct in public office. As the ICSO currently does not provide for any criminal sanctions, Hon James TO's proposal to introduce criminal sanctions into the ICSO, if implemented, would represent a major departure from the existing regulatory regime. Also, the proposal is not amongst the first Commissioner's recommendations.

**Clause 20 - Section 65(a)**

15. Hon James TO's proposed amendment seeks to amend clause 20 of the Bill. In addition to the new section 65A proposed by the Administration in clause 20, Hon James TO's proposed amendment seeks to introduce the following requirements -

- (a) the head of the department concerned shall report to the Commissioner "the times of the [officer-in-charge] has notice of the revocation and of discontinuance [of the interception or covert surveillance concerned]";
- (b) when the officer-in-charge of the interception or covert surveillance concerned has notice of the revocation of the prescribed authorization, he "shall not use (for investigative operations) or gain access to any protected product obtained after the revocation"; and
- (c) contravention of (b) above shall be an offence punishable with a maximum penalty of 2 years' imprisonment.

(the proposals above are referred to hereunder as "proposal (a)", "proposal (b)" and "proposal (c)" respectively)

16. The first Commissioner raised concerns regarding the "unauthorized" operations resulting from the time gap between the revocation of a prescribed authorization and the actual discontinuance of the operation, which is technical and unavoidable. Clause 20 of the Bill is intended to address this technical problem. It adds a new section 65A to provide that (i) if a prescribed authorization is revoked by the relevant authority in whole or in part, the LEA must make arrangements to ensure the discontinuance of the interception or covert surveillance in question as soon as reasonably practicable; and (ii) any protected products obtained during the time gap are to be regarded as having been obtained pursuant to a prescribed authorization for the purposes of the ICSO so that these products would have to be protected from unauthorized use

or disclosure and be disposed of in accordance with the provisions of the ICSO.

17. We consider that proposals (a) and (b) concern operational details and should be incorporated in the CoP rather than in the legislation. The CoP is promulgated pursuant to section 63 of the ICSO, and serves to provide practical guidance to LEAs on the principles and requirements set out in the ICSO. Non-compliance with the CoP has to be reported to the Commissioner, and the officers concerned would be subject to disciplinary action or, depending on the circumstances of the case, may be prosecuted for the common law offence of misconduct in public office.

18. Proposal (c) provides for criminal sanctions in cases of using (for “investigative operations”) or gaining access to any protected product obtained after the revocation of a prescribed authorization. The Administration’s position regarding the introduction of criminal sanctions under the ICSO is already detailed in paragraphs 13 and 14.

**Clauses 6(2), 8(2), 9, 16(10), 17(5) and 18; New Clauses 21 and 22**

19. Hon James TO’s proposed amendment seek to (i) replace “any provision of this Ordinance” in clauses 6(2), 8(2), 16(10) and 17(5) with “under those terms referred to in section 29(1) to (5) as well as any further authorization granted under section 29(6) or (7) or section 30 of this Ordinance”; (ii) replace “any provision of this Ordinance” in clause 9 with “section 29(6) or (7) or section 30 of this Ordinance”; and (iii) replace “any provision of this Ordinance” in clause 18 with “under those terms referred to in section 29(1) to (5) as well as any further authorization granted under section 29(6) or (7) or section 30 of this Ordinance”. Since the same phrase also appears in sections 32 and 38 of the ICSO, Hon James TO also proposed consequential amendments to the two aforementioned sections by adding new clauses 21 and 22.

20. The existing section 32 of the ICSO provides that a prescribed authorization may be issued or renewed subject to any conditions specified in it that apply to the prescribed authorization itself **“or to any further authorization or requirement under it (whether granted or imposed under its terms or any provision of this Ordinance)”**. Thus, conditions may be imposed by the relevant authority when it issues or renews a prescribed authorization, and the expression **“any further authorization or requirement under it”** in section 32 refers to any authorization or requirement granted or imposed under the terms of the prescribed authorization in question such as those referred to in section 29(1) to (5) as well as any further authorization granted under section 29(6) or (7) or section 30 of the ICSO. Paragraph 129

of the CoP requires that where conditions are imposed, the officers must ensure that they are observed in executing the prescribed authorization.

21. On the recommendation of the first Commissioner, we propose that the relevant authority should have a similar power to impose new conditions in other scenarios. Section 24 deals with the determination of an application for confirmation of an emergency authorization while section 27 deals with the determination of an application for confirmation of a prescribed authorization or renewal issued or granted upon an oral application. In line with section 32, the proposed sections 24(3A) and 27(3A)(b) aim to make it clear that any new conditions imposed by the panel judge or the relevant authority may apply not only to the emergency or prescribed authorization itself but also to any further authorization or requirement under it.

22. Likewise, the new sections 57(5A)(b), 58(3A)(b) and 58A(6)(b) are proposed for a similar purpose. Whenever a prescribed authorization is only partially revoked following the discontinuance of the interception or covert surveillance, arrest of the subject, or in case of material inaccuracy or change in circumstances, the relevant authority may impose new conditions that apply not only to the prescribed authorization itself but also to any further authorization or requirement under it.

23. The existing section 38 of the ICSO provides that a device retrieval warrant may be issued subject to any conditions specified in it that apply to the warrant itself or to any further authorization under it (whether granted under its terms or any provision of the ICSO). In line with section 38, the proposed section 38A(4)(b) seeks to make it clear that in a situation where a device retrieval warrant is not revoked or is only partially revoked, the panel judge may impose new conditions which apply to the warrant itself or to any further authorization under it. Such “further authorization” refers to any authorization granted under section 36 or 37 of the ICSO.

24. Having regard to section 32 of the ICSO, which provides that a prescribed authorization “may be issued or renewed subject to any conditions specified in it that apply to the prescribed authorization itself or to any **further authorization or requirement under it** (whether granted or imposed under its terms or any provision of this Ordinance)” (**emphasis added**), we consider it appropriate to maintain consistency by retaining the use of “further authorization or requirement under it” in the relevant clauses. In the past nine years since the enactment of the ICSO, neither the panel judges nor any authorizing officers have experienced any difficulties in understanding or exercising their powers under section 32. The first Commissioner has not made any recommendation that section 32 should be amended.

Other Issues Raised in the Meetings on 9 and 16 November 2015

To explain the term “becomes aware” as opposed to “knows” in the proposed section 58A of the ICSO (clause 18 of the Bill)

The proposed new section 58A provides that if, while a prescribed authorization is in force, the officer concerned who is for the time being in charge of the interception or covert surveillance concerned **becomes aware** that there is a material inaccuracy in the information provided for the purpose of an application under section 8, 11, 14, 17, 20, 23(1) or 26(1), or there has been a material change in the circumstances on the basis of which the prescribed authorization was issued, renewed or confirmed, the officer must as soon as reasonably practicable after **becoming aware** of any of the aforesaid matter, cause a report on the matter to be provided to the relevant authority by whom the prescribed authorization was issued, renewed or confirmed.

2. The expression “**becomes aware**” has been used in the existing sections 57 and 58 of the ICSO. “**Become aware**” and “**know**” are not defined in the Interpretation and General Clauses Ordinance (“IGCO”) (Cap. 1) or the ICSO. For the purpose of the existing sections 57 and 58 and the proposed section 58A, we do not consider that there is any material difference between the two expressions in terms of achieving the policy intent. The use of “*becomes aware*” in the current context has the effect of emphasising that the officer comes to know that the relevant circumstances or information exists from a certain point of time. Section 58 is about reporting to the relevant authority following the arrest of the subject. Operationally, when section 58 is invoked, the officer concerned would verify the information pertinent to the arrest using the established internal checking system before he provides the relevant authority with a report under section 58(1).

3. As regards the Chinese equivalent of “**becomes aware**”, the expression “知悉” has been used in various ordinances. Recent examples can be found in section 8(1) and (2) of the Lifts and Escalators (General) Regulation (Cap. 618, sub. leg. A) and section 7(1) and (2) of Schedule 7 to the Competition Ordinance (Cap. 619).



**To explain the relevance of the review on interception and covert surveillance by non-public officers to the question of whether criminal sanctions should be imposed under the ICSO**

4. The ICSO has put in place an elaborate system to regulate the conduct of interception of communications and covert surveillance by public officers of specified departments. Pursuant to section 63 of the ICSO, the Secretary for Security has promulgated a detailed Code of Practice (“CoP”) that provides practical guide to public officers of the specified departments. Officers are reminded to comply with the ICSO and the CoP at all times. All non-compliance has to be reported to the Commissioner on Interception of Communications and Surveillance who performs an oversight function.

5. Within the departments concerned, there are comprehensive guidelines governing the procedures and conduct of covert operations, and officers who have committed misconduct are subject to disciplinary action. A public officer who wilfully conducted interception or covert surveillance without a prescribed authorization may have committed the common law offence of “misconduct in public office” and if convicted, is punishable by 7 years’ imprisonment. Since the enactment of the ICSO, disciplinary actions have been taken against about 60 officers who were found in breach of the ICSO, the CoP and/or related internal guidelines.

6. In the recent past, the Commissioner was generally satisfied with the overall performance of the LEAs and their officers in their compliance with the relevant requirements. Although there have been cases of individual officers failing to comply with the requirements, there are no signs of the officers flouting the law or deliberately disregarding the requirements.

7. Between 1996 and 2006, the Law Reform Commission (“LRC”) published five reports relating to privacy, including two on “Regulating the Interception of Communications” and “The Regulation of Covert Surveillance” respectively (the “two LRC reports”). In the light of the recommendations relating to interception and covert surveillance conducted by public officers in the two LRC reports, the Government introduced the ICSO in 2006 to regulate the interception and covert surveillance operations conducted by the public officers. On the regulation of similar operations or activities by non-public officers, the responsible policy bureau is still considering the relevant recommendations. We consider that the question of whether criminal sanctions should be introduced under the ICSO has to be considered holistically alongside with the relevant bureau’s deliberation on non-public officers conducting similar operations or activities. Pending completion of such

deliberation, we do not have plans to consider imposing criminal liability on public officers under the ICSO.

**To explain the legal basis on which the Commissioner may make written notes and summaries when he is checking protected products**

8. As explained in the Annex to LC Paper No. CB(2) 214/15-16(01), section 40(1) of the IGCO provides that where any Ordinance confers upon any person power to do or enforce the doing of any act or thing, all such powers shall be deemed to be also conferred as are reasonably necessary to enable the person to do or enforce the doing of the act or thing. Insofar as the making of written notes and summaries of protected products is reasonably necessary to enable the Commissioner and his delegated staff to conduct reviews, carry out examinations and examine protected products, they can rely on the general incidental power under section 40(1) of the IGCO to make such notes and summaries when performing these functions.

**To explain whether the Commissioner can order the relevant LEA to retrieve a surveillance device after expiry of the prescribed authorization concerned**

9. The Commissioner and the panel judges perform different functions under the ICSO. Whilst the Commissioner is an independent authority responsible for overseeing the compliance by the LEAs and their officers with the relevant requirements, the panel judges are the authorities to consider applications for prescribed authorization to conduct interception and covert surveillance. A prescribed authorization also authorizes, among others, the retrieval of any of the devices authorised to be used under the prescribed authorization. The panel judges are also the authorities to issue a device retrieval warrant authorizing the retrieval of any of the devices used under a prescribed authorization after such authorization has expired.

10. Under section 42(1) of the ICSO, the Commissioner shall notify the head of an LEA of his findings in a review of the LEA's compliance with the relevant requirements. Under section 52(1), if, in the course of performing any of his functions, the Commissioner considers that any arrangements made by an LEA should be changed to better carry out the objects of the Ordinance or the provisions of the CoP, he may make such recommendations to the head of the LEA as he thinks fit. Where the Commissioner notifies the head of an LEA of his findings under section 42(1) or makes any recommendations to the head of an LEA under section 52(1), the head of the LEA shall submit to the Commissioner a report with details of any measures taken by the LEA (including any disciplinary action taken in respect of any officer) to address any

issues identified in the findings or to implement the recommendations, as soon as reasonably practicable or within the time specified by the Commissioner.

11. As explained in the Annex to LC Paper No. CB(2) 214/15-16(01), the CoP already stipulates that surveillance devices should not be left in the target premises after a covert surveillance operation. Wherever practicable, a surveillance device should be retrieved during the period of authorization. Where it is not reasonably practicable to do so, the LEA must apply for a device retrieval warrant. Any decision of not applying for a device retrieval warrant where the device has not been retrieved after the expiry of an authorization should be endorsed by an officer at the directorate rank, and a report on the decision, together with the reasons and steps taken to minimize possible intrusion into privacy by the device, should be submitted to the Commissioner. The Commissioner may then carry out a review based on the information provided and reasons advanced. If the Commissioner is not satisfied with an LEA's reasons and considers that the device should have been retrieved before or after expiry of the authorization, he may notify the LEA of his findings under section 42 or make a recommendation to the LEA under section 52, and where appropriate, recommend the LEA to take appropriate actions, including applying to a panel judge for a device retrieval warrant. The LEA concerned shall then submit to the Commissioner a report with details of any measures taken by the department to implement the recommendations as soon as reasonably practicable or within the time specified by the Commissioner.

**To explain the mechanism for the destruction of intelligence derived from interception or covert surveillance operations of which the prescribed authorization has been revoked on the ground of material inaccuracy in the information provided in the application concerned**

12. As explained in the Annex to LC Paper No. CB(2) 214/15-16(01), information obtained from covert operations, together with the information obtained by an LEA from other sources such as crime reports from the public, case investigation and open source materials, can be aggregated into intelligence after being screened, evaluated and analysed. Such intelligence will be used by the LEA for the purpose of crime prevention or detection. The intelligence management system of an LEA is subject to tight control. LEAs have strict internal guidelines requiring that intelligence must be gathered through legitimate means, and is regularly reviewed.

13. Under section 64 of the ICSO, a prescribed authorization is not affected by any minor defect relating to it. Any information (including any protected product) obtained pursuant to a prescribed authorization is not by reason only of any minor defect relating to the prescribed authorization to be

rendered inadmissible in evidence in any proceedings before any court. However, if the relevant authority, upon receipt of a report of any material inaccuracy or material change in circumstances, considers that the conditions for the continuance of the prescribed authorization (or any part thereof) under section 3 of the ICSO are not met, he is, under the proposed new section 58A, obliged to revoke the prescribed authorization (or that part of the prescribed authorization). The revocation will not have any retrospective effect on the validity of the prescribed authorization prior to its revocation. Any protected products obtained before the revocation are still considered to have been lawfully obtained pursuant to a prescribed authorization. Like any other protected products, they will have to be dealt with in accordance with the provisions of the ICSO, including section 59 which sets out the safeguards and destruction arrangement for protected products.

***To refine the drafting of the Code of Practice (CoP) in relation to “time gap”***

14. Having regard to Members’ views, we have refined the drafting of the three paragraphs to be added to the CoP in relation to “time gap”. The revised paragraphs are at **Attachment**.

## Attachment to Appendix III

### Amendments to the ICSO Code of Practice

*(Revisions marked in underscored bold)*

- [ ]. *Where a prescribed authorization has been revoked by the relevant authority under relevant provisions of the Ordinance, the officer-in-charge must take immediate action to cause the interception or covert surveillance operation to be discontinued as soon as reasonably practicable. However, due to the time required for the communication of the revocation decision to the officers responsible for discontinuing the operation, there is inevitably a time gap between the revocation of the prescribed authorization and the actual discontinuance of the operation.*
- [ ]. *Under section 65A(1) of the Ordinance, if a prescribed authorization or a part of a prescribed authorization is revoked under section 24(3)(a)(i), 27(3)(a)(i), 58(2) or 58A(4) of the Ordinance, the head of the department concerned must make arrangements to ensure that the interception or covert surveillance concerned or the relevant part of the interception or covert surveillance concerned is discontinued as soon as reasonably practicable. **The time of revocation for each case should be clearly documented.** Any interception or surveillance products obtained after the revocation but before the actual discontinuance of the interception or covert surveillance are deemed to have been obtained pursuant to a prescribed authorization for the purposes of the Ordinance. In other words, these products will have to be dealt with in accordance with the provisions of the Ordinance, including section 59 which sets out the safeguards for protected products. As soon as an officer has notice of the revocation, the officer shall not use or gain access to any **protected** products **(including its copy)** obtained during the time gap **for the purpose of investigation or any other purpose.***
- [ ]. *Whether the time taken to discontinue the operation is reasonable or not depends on the particular circumstances of the case. As a practical guidance for the departments to comply with the requirement that the interception or covert surveillance must be discontinued “as soon as reasonably practicable”, the benchmark timeframe within which discontinuance should normally be effected is 60 minutes counting from the time of revocation by the relevant authority. **In any event, the time of revocation and t**~~The time of~~*

discontinuance ~~should~~ **must** be reported to the Commissioner. Any department which cannot discontinue the operation within the above benchmark timeframe ~~should~~ **must** also explain the reasons when reporting **the time of revocation and** the time of discontinuance to the Commissioner. The Commissioner will review whether the time taken is reasonable or not.