For information
6 April 2006 **SB Ref: ICSB 3/06**

Bills Committee on
Interception of Communications and Surveillance Bill

Response to issues raised by Members
at the meeting of 25 March 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Bills Committee on 25 March 2006.

Response to issues raised

Issue 1 : Legal professional privilege (LPP)

- ***To explain, quoting the relevant provisions in the Bill, how LPP would be safeguarded, and consider reflecting the right to confidential legal advice provided in Article 35 of the Basic Law in clause 56(1)(c) of the Bill.***

2. At present law enforcement agencies (LEAs) do not knowingly seek to obtain information subject to LPP, whether by interception of communications, covert surveillance or other means, except where there is a statutory exemption. Officers of our LEAs have been fully briefed on the legal requirements in this regard and will seek legal advice when in doubt.

3. Under the Bill, information that may be subject to LPP is given special protection. The relevant clauses are as follows –

(a) Clause 2(3) :

"For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of "Type 2 surveillance" in subsection (1) is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege will be obtained by carrying it out."

The effect of the provision is that applications for all covert operations under the Bill that may involve LPP (including Type 2 surveillance operations which, in normal circumstances, are to be authorized by the executive authorities), should be considered by panel judges, who can be expected to be conscious of the principles governing LPP.

(b) Paragraph (b)(viii) of Part 1 of Schedule 3 and paragraphs (b)(ix) of Parts 2 and 3 of Schedule 3 :

"An affidavit supporting an application for the issue of a judicial authorization for interception is to –

(a) …

(b) set out –……

(viii) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the interception"

"An affidavit supporting an application for the issue of a judicial authorization for Type 1 surveillance is to –

(a) …

(b) set out –……

(ix) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the Type 1 surveillance"

"A statement supporting an application for the issue of an executive authorization for Type 2 surveillance is to –

(a) …

(b) set out –

(ix) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the Type 2 surveillance"

These requirements would have the effect of compelling LEAs to assess the likelihood of interference with LPP so that the authorizing authority could make an informed decision on whether authorization should be granted. For an operation

that would otherwise be Type 2 surveillance but where information which may be subject to LPP is likely to be obtained, clause 2(3) would then apply so that the application would have to be made to a panel judge instead. The assessment of the likelihood of information that may be subject to LPP being obtained would also facilitate subsequent reviews by the Commissioner on Interception of Communications and Surveillance (the Commissioner) on whether the appropriate authorization has been sought.

(c) Clause 3 :

"*(1) In this Ordinance, the conditions for the issue or renewal, or the continuance, of a prescribed authorization, are that, in the circumstances of the particular case –*

(a) …

(b) the interception or covert surveillance is proportionate to the purpose sought to be furthered by carrying it out, upon –

(i) balancing, in operational terms, 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

(ii) 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.

(2) In this section, "relevant factors" means –

(a) the immediacy and gravity of [the serious crime to be prevented or detected or the particular threat of public security]; and

(b) the likely value and relevance … of the information likely to be obtained…".

In his consideration of the application by applying the tests of proportionality and hence necessity, the panel judge would

take into account the impact on LPP in deciding whether the proposed operation is proportionate to the purpose sought to be furthered by carrying out the operation.

(d) Clause 31 :

"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)."

A panel judge may prescribe such conditions as he considers appropriate in the case. He may, therefore, prescribe conditions to minimize possible interference with information which may be subject to LPP.

(e) Clause 56(1) :

"(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;……

(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."

The extent to which interception or surveillance product may be disclosed should be kept to the minimum necessary and the protected product has to be destroyed as soon as its retention is not necessary. In practice, any information obtained in the

course of a duly authorized operation that is found to be subject to LPP remains privileged, and such information cannot be used for any law enforcement purposes. The disclosure and retention of the relevant products would not be necessary unless, for covert surveillance products, it is necessary to retain them for the prosecutor to carry out his duty to ensure a fair trial in a future proceeding. The effect of the inadvertent interference with LPP, if any, would be kept to a minimum. The compliance with the clause is also subject to review by the Commissioner.

4. Given the design of the scheme, in practice, we envisage that interception of communications or covert surveillance which has a relatively higher of likelihood of inadvertently making available information subject to LPP would only arise where the lawyer himself is criminally involved in an alleged offence, and hence the relevant communications sought would likely not be protected by LPP. In the course of carrying out the covert operation on the lawyer, e.g. by intercepting his telephone conversations, the LEA may inadvertently pick up other information that is subject to LPP. In other cases, we do not envisage that an authorization to, for example, intercept a lawyer's telephone or place a listening device in his office would be viewed as proportionate, and an application would unlikely be made in the first place. Where the lawyer is the target, the panel judge may also impose appropriate conditions under clause 31 of the Bill to protect information subject to LPP.

5. We consider that the present scheme is consistent with Article 35 of the Basic Law. Nonetheless, taking into account Members' views, we will consider whether clause 56(1) should make an express reference to LPP materials.

- ***To consider requiring LEAs to report to the panel judge for each judicial authorization relating to LPP after a specified period.***

6. The key safeguard for information subject to LPP that is inadvertently obtained is to limit disclosure of the material and to ensure its destruction as soon as possible. Clause 56(1) of the Bill should achieve this. To retain the material for third parties to further check it does not add to the protection. The safeguards built in the proposed regime should afford sufficient protection to ensure that information

subject to LPP that may be inadvertently obtained is not disclosed or used by the LEAs, and is destroyed as soon as possible unless the products have to be kept for the prosecutor to carry out his duty to ensure a fair trial in a future proceeding. (Please see paragraph 3(e) above.) The Commissioner would ensure compliance in this regard. We do not consider it necessary or indeed desirable to impose on LEAs the requirement to report back to the panel judge as this would unnecessarily overburden him without adding to the safeguards.

Issue 2 : Public security

- ***To provide information, if available, on why a definition for "public security" was not proposed in the 1996 Law Report Commission report on interception of communications and the 1997 White Bill on Interception of Communications.***

7. As far as we are aware, no explanations were provided at the time as to why the term was not defined.

- ***To consider providing a definition for the term "public security" in the Bill or stating the exclusions from it.***

8. The Administration has explained in its paper for the meeting held on 25 March 2006 (SB Ref: ICSB 2/06) and at the meeting the difficulty of giving the term "public security" an exhaustive definition.

9. As for the proposal for the Bill to stipulate exclusions, we reiterated at the meeting on 25 March 2006 that the public security ground would not be used for political purposes, nor for suppressing the guaranteed right of freedom of expression or peaceful advocacy. Members also discussed the provisions in some jurisdictions defining such exclusions, and noted the difficulties arising from such provisions. Having said that, we note the advice from Members that we should try to formulate an exclusion provision. We will now work actively to see if we could come up with a provision that we could recommend to Members. We shall revert to Members on the outcome of our work.

Issue 3 : To consider setting out expressly the consequence for law enforcement officers in breach of the provisions in the Bill.

10. As set out in previous papers submitted to the Panel of Security

and the Bills Committee (SB Ref: ICSB 01/06) (extract at **Annex**), LEA officers who fail to comply with the new legislation would be subject to disciplinary action or, depending on the cases, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law.

11. We have carefully considered the desirability of stipulating in the Bill the consequence of any breach of provisions of the Bill (as well as the Code of Practice to be issued by the Secretary for Security under clause 59 of the Bill or conditions set out in the authorization concerned). We do not consider it appropriate to do so. This is because the circumstances of each case, and hence any non-compliance, would differ. In cases warranting disciplinary action (rather than instituting criminal proceedings), the range of such actions could vary significantly – from verbal warning at one extreme for minor breaches to dismissal at the other extreme for very serious breaches, and there are existing mechanisms in respect of the procedural matters relevant to such actions. It is not possible to set out exhaustively in the law the full range of possible consequences of such breaches as well as the applicable procedures.

12. Nonetheless, we appreciate the need to make it abundantly clear to LEA officers (and, for transparency, to the public) the serious consequence of any breach of the relevant requirements. The Bill specifically provides for the promulgation of a Code of Practice for such covert operations, and we shall include provisions in the Code to clearly set out the possible consequence of such breach. The Code would be published and made public.

13. Furthermore, under the Bill, the Commissioner would already be apprised of actions to be taken by the LEAs in respect of non-compliance. The head of the LEA concerned is also required to provide a report with details of any measures taken by the department concerned to address any of the issues arising from the decision of the Commissioner following his reviews or his examinations pursuant to complaints. We envisage that these details may include, where applicable, actions by the department in respect of the officers concerned.

Issue 4 : Appointment of the panel of judges

- ***To provide information on the authorization authorities for***

interception of communications or surveillance and details of their regime for granting such authorizations in other common law jurisdictions and whether integrity checking was conducted on judges in such jurisdictions.

14. The practice varies, as follows –

- UK
  - Interception operations are authorized by the Secretary of State.
  - Intrusive surveillance operations are authorized by the Secretary of State or one of the "senior authorizing officer" listed in the Regulation of Investigatory Powers Act 2000, and approved by a Surveillance Commissioner.
  - Directed surveillance operations are authorized by officers of public authorities designated by the Secretary for State.
- Australia
  - Interception of telecommunications : For criminal investigation cases, an eligible judge, or a member of the Administrative Appeals Tribunal nominated by the Minister. For security cases, the Attorney-General.
  - Inspection of postal articles : In relation to articles on which customs duty is payable and articles believed to contain controlled drugs, a customs officer / a senior customs officer / an Australia Post employee appointed by Australia Post. For security cases, the Minister.
  - Covert surveillance : For criminal investigation cases, an eligible judge, or a member of the Administrative Appeals Tribunal nominated by the Minister. But the use of tracking devices not involving entry onto premises without permission or interference with the interior of a vehicle without permission is authorized by an appropriate authorizing officer. For security cases, the authorization is made by the Minister.

- US

  - Interception of telecommunications and covert surveillance : For criminal investigation cases, the order is granted by a judge of competent jurisdiction. For foreign intelligence cases (a) the order is granted by one of the 11 judges of the Foreign Intelligence Surveillance Court; or (b) is authorized by the President, through the Attorney General, without court order if the operations are directed at communications between foreign powers.

  - Inspection of postal articles : Any judge.

15. There is little public information on details of security vetting arrangements of other jurisdictions. It is clear that similar to our system, other jurisdictions classify information and impose various controls over the personnel with access to such information. Such controls typically include various forms of security checking / vetting / clearance conducted on the personnel, at levels corresponding to the sensitivity of the information which the personnel are allowed to access. However, as far as we are aware there is little public information on details such as specifically which positions, whether judicial or non-judicial positions, are required to undergo which level of vetting, or details of what different levels of vetting entail. With specific reference to judges, we understand that in the United States, all federal judges are subject to "security check" conducted by the Federal Bureau of Investigation before their appointment.

- ***To advise whether persons who have undergone integrity checking would be informed of the results of the checking and, if not, the reasons for not doing so.***

16. As explained at the Bills Committee meeting on 25 March 2006, as a general arrangement, the results of the checking will be passed to the appointment authority. It remains a conscious assessment and decision by the appointment authority as to whether a particular individual should be appointed, having regard to the outcome of the checking and other relevant considerations such as the nature of and the possible impact on the duties to be performed by the appointee. It falls on the appointment authority to consider whether to inform the candidate of the detailed

reasons. In some cases, to do so could compromise the confidentiality of information provided by others. We see no reasons for deviating from the above general arrangements in respect of the panel judges, the Commissioner and their respective staff in our proposed regime.

Security Bureau
April 2006

Annex

Interception of Communications and Covert Surveillance

Sanctions

Relevant extracts from the Paper SB Ref: ICSB 1/06

22. Apart from the issue of notification of targets covered in para. 19 above, the Panel has in this context asked about sanctions for non-compliance and whether the code of practice would be subsidiary legislation. We have explained that LEA officers who fail to comply with the new legislation would be subject to disciplinary action or, depending on the cases, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law. The code of practice would be published, but would not be subsidiary legislation. The relevant extracts of the Administration's response are at **Annex A9**.

* * * * * *

[Re: Annex]

Annex A9 to Paper SB Ref: ICSB 1/06

Interception of Communications and Covert Surveillance

Sanctions and Code of Practice

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 8 : To advise on the consequences of illegal covert surveillance conducted by law enforcement agencies.

Item 9 : To consider adding penalty provisions for non-compliance with any code of practice made under the proposed legislation.

14. We have proposed that the current exercise be limited to Government entities. This means that non-Government parties would not be subject to the regulation proposed. It would create an anomaly if, for the same conduct, law enforcement officers but not others would be subject to a new criminal offence. We will consider the need for introducing new criminal offences at the next stage. Under our proposal, a breach under the proposed legislation would be subject to disciplinary action, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorization might also commit the common law offence of misconduct in public office. In addition, any non-compliance would be subject to the scrutiny of the Commissioner, who may report such cases of irregularity to the heads of department and to the Chief Executive (CE), and who would handle complaints. Statistics on such cases would also be provided to CE in the Commissioner's annual report, which would be tabled in LegCo. These are powerful measures to ensure that LEAs and their officers will comply with the law and the applicable procedures.

15. Separately, all public officers have to observe the full range of existing laws. For example, the Telecommunications Ordinance provides for various offences in relation to the wilful interception of messages (sections 24) and damaging telecommunications installations with intent (section 27). The Post Office Ordinance has provisions governing the unauthorized opening of postal packets (sections 27 and 29). Other laws such as the Personal Data (Privacy) Ordinance may also be relevant. For a fuller summary of existing laws that may be applicable, please see Chapter 2 of the 1996 LRC report.

Item 10 : To advise whether the code of practice made under the legislation is subsidiary legislation.

16. The basic principles of the regime would be set out in the law. Amendments to these would necessarily have to be passed by LegCo. We do not consider it advisable for the Code of Practice covering operational details, which may need to be changed from time to time, to be made statutory. Our proposed legislation would stipulate that the Commissioner may make recommendations to the Secretary for Security on the Code or propose amendments thereto, thereby providing a considerable degree of oversight in respect of the content of the Code. Furthermore, the Code would be published and hence subject to public scrutiny.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security 21 February 2006

Item 3 : To explain whether non-compliance with any code of practice made under the proposed legislation without legal consequences would respect the provisions in Article 30 of the Basic Law (BL30).

7. Under BL30 –

- "The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents"

- "except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."

For reasons we have explained in previous discussions, we propose that for the current exercise we focus on the second part of BL30 (regulation of operations by LEAs). To fully implement BL30 we will need further work separately on the first part of BL30.

8. While the first part of BL30 requires that the freedom and privacy of communication of Hong Kong residents shall be protected by law, it does not mandate that such protection must be in the form of criminal sanctions. In previous papers which the Law Reform Commission (LRC) has published, the LRC has identified various activities that might infringe upon privacy, and proposed a combination of criminal and civil sanctions against such activities, applicable to all

persons in Hong Kong. If after the necessary discussions in our society it is decided to enact legislation on any of such proposed criminal and civil sanctions, such sanctions would apply to LEA officers.

9. Under our proposed regime, we have included very powerful sanctions against non-compliance. A breach under the proposed legislation would be subject to disciplinary proceedings, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorization might also commit the common law offence of misconduct in public office. Any non-compliance would be subject to the Commissioner's oversight. The Commissioner would also be able to refer any irregularity to the respective head of department, the Chief Executive or the Secretary for Justice. Separately, like everyone in Hong Kong, all public officers have to observe the full range of existing laws.

* * * * * *