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

Bills Committee on Interception of Communications and Surveillance Bill

Administration's Response to Issues Raised by the Senior Assistant Legal Adviser, Legal Service Division, Legislative Council Secretariat in his letter of 10 April 2006

Clause 2 - Interpretation

In the definition of "head", what does "any deputy of the head of the department" mean? Is there any inconsistency between the English and Chinese texts?

Clause 2 provides that the term "head", in relation to a department, includes any deputy of the head of the department. This means, for example, the head of the Police includes the Commissioner of Police and the two Deputy Commissioners of Police. Apart from providing more flexibility to the departments in their fulfilment of the various functions and requirements under the Bill, it would minimize the need for the head of the department to handle cases in which he has made a prior decision.

2. There is no inconsistency between the Chinese and English texts.

In Clause 2(2), why is there no reasonable expectation of privacy in relation to any activity carried out in public place?

3. Clause 2(2) of the Bill provides that a person is not regarded as being entitled to a reasonable expectation of privacy in relation to any activity carried out by him in a public place. As explained in our reply of 1 April 2006 to the Bar Association, the term "activity" has been chosen to be clearly distinct from that of "words spoken" in the context of the Bill – with the latter used in the definition of "listening device" and the former used in the definition of "optical surveillance device" and further with both used as distinct references in paragraph (a) of the definition of "Type 2 surveillance". The clear intention is that this

would only cover activities in the public as opposed to words spoken.

4. Activities carried out in public places would be visible to any members of the public, and there should therefore be no reasonable expectation that such activities are not being observed. For law enforcement purposes, the provision makes it clear that no authorization is required for using optical surveillance device for operations involving observation in public places. This would however not affect the rights of the person for other purposes (including privacy of communication). If necessary, we may include further provisions to make the point more express.

In Clause 2(5), what is "data produced in association with the communication"?

5. Clause 2(5) provides that "for the purposes of this Ordinance, the contents of any communication transmitted by a telecommunications system include any data produced in association with the communication". Data produced in association with the communication include, for example, the telephone number dialled for a telephone call, the email address of the sender/recipient of an email, etc.

In Clause 2(7), who is the person to act in or perform the function of panel judges when he is no longer holding office or unable to perform the functions of such office? Does that person need to be appointed by the Chief Executive and subject to integrity checking? What is the purpose of this sub-clause insofar as a panel judge is concerned?

6. This clause caters for the difference between "a" panel judge and "the" panel judge. The same panel judge may not be considering the same case, e.g., between the making of an oral application and its subsequent confirmation, or between the retirement from and new appointments to the panel, or when a panel judge is temporarily out of town or otherwise unavailable. In these and similar cases, another panel judge would have to perform his functions. As the clause refers to "the person for the time being holding such office or appointed to act in or perform the functions of such office or lawfully performing the functions of such office" and "the person for the time being appointed to act in or perform the functions of such office or lawfully performing the functions of such office", it works by reference to a person who ***has been***

appointed to hold the office or appointed to act in or perform the functions of the relevant office. Thus, it does not affect the appointment provisions and procedures already included in the Bill.

Clause 3 - Conditions for prescribed authorization

What is the difference between "public security" and "public safety or security" used in the Executive Order? What are the scope and nature of matters intended to be covered by the term "public security"? We enclose for your reference the definition of "terrorist act" in the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575). Would the Administration consider the drafting approach in that definition assist the concern of Members for a clear definition?

7. Please see the Administration's response set out in the paper presented for information of the Bills Committee meeting on 19 April 2006 (SB Ref: ICSB 5/06). As explained in that paper, the drafting approach for the definition of "terrorist act" is not appropriate for the term "public security".

How would a panel judge assess "in operational terms" under Clause 3(1)(b)(i)?

8. The reference to "operational terms" is included to ensure that the authorizing authority does not consider the proposed authorization in isolation, but as part of an overall operation. Since no two cases are identical, at the end of the day, there would inevitably be some exercise of judgement having regard to the circumstances of the case. Hence the reference to "in operational terms". The onus is on the law enforcement agencies (LEAs) making the application to justify that the operation is proportionate. The LEAs would have to provide the necessary information concerning the proposed operation to the panel judge.

Clause 4 - Prohibition on interception

What kind of telecommunications transmitted by radiocommunications are intended to be covered and excluded by Clause 4(2)(b)?

9. The effect of clause 4(2)(b) is to exclude "any interception of telecommunications transmitted by radiocommunications (other than the radiocommunications part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under the Telecommunications Ordinance (Cap. 106))" from the coverage of the Bill. In other words, interception of radiocommunications in general, e.g., the transmission of radio and television broadcast signals, would not fall under the regime under the Bill. However, if such radiocommunications is part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under Cap. 106 (e.g. public mobile phone services), its interception would need authorization under the Bill in order to protect communications for general users.

Please set out the types of interception under other enactments referred to in Clause 4(2)(c).

10. Clause 4(2)(c) would exclude from the coverage of the Bill any interception authorized, permitted or required to be carried out by or under any enactment other than the Bill. Some examples of such enactments, as referred to in the 1996 Report of the Law Reform Commission on interception (other than those under the Telecommunications Ordinance and the Post Office Ordinance) are –

- Bankruptcy Ordinance (Cap. 6), section 28
- Prison Rules (Cap. 234, sub. leg. A), Rules 47 and 48
- Mental Health Regulations (Cap. 136, sub. leg. A)
- Import and Export Ordinance (Cap. 60), section 35(3)

11. For the avoidance of doubt, the clause also expressly excludes any use of search warrants which might otherwise fall under the definition of interception under the Bill.

Clause 6 - Panel judges

Schedule 2 - Procedures of and other matters relating to panel judge

Since it is possible to apply for judicial review of decisions of eligible judges, would there be integrity checking of those judges hearing the

judicial review and any appeal of the review?

12. We do not consider it necessary to apply extended checking to the judge hearing the judicial review or any subsequent appeal on the decision of panel judges for the following reasons –

- The number of such cases is expected to be much smaller, and the extent and frequency of the judges having to access sensitive information through hearing the judicial review or subsequent appeals would correspondingly be much less, than the panel judges.
- More importantly, such cases are only expected to arise when the covert surveillance / interception operation is already known to the target, either when the product is produced as evidence in proceedings against the target, or when the complaint of the target to the Commissioner is substantiated. As explained in our earlier papers, at such a stage the covert operation would have already turned overt, and hence the sensitivity of the information involved would be much less than before or during such operations.

In Clause 6(2), is reappointment also on the recommendation of CJ?

13. It is our intention that reappointment of the panel judges will follow the procedure for appointment – i.e., the reappointment will be made by the Chief Executive (CE) on the recommendation of the Chief Justice (CJ). If necessary, we may include further provisions to make this more express.

Under section 4 of Schedule 2, is there any conflict for a panel judge to act judicially when he is performing a non-judicial function?

14. The term "act judicially" is explained in the Administration's paper SB Ref: ICSB 5/06. In essence, the requirement for the panel judge to "act judicially" means that the judge would have to exercise his power without bias and fairly weigh the competing considerations of privacy on the one hand and law enforcement on the other, and to consider the applications submitted to him on the strength of evidence that is placed before him, rather than acting as an administrator and basing his decision on administrative and policy considerations. We see no conflict for the panel judge to act judicially while not sitting as a court.

Clause 8 - Application for judicial authorization

Is there any prohibition against making an application to another panel judge if a previous application has been refused? Has the Administration considered whether there is any need requiring reference to previous application being made?

15. As with provisions in other legislation on applications for authorization in general, the Bill does not expressly prohibit making an application again after a previous application has been refused. This is for good reason – the circumstances may have changed or new information is available, for example. A re-submission should not therefore be seen as abuse of process. We envisage that the Commissioner would also pay special attention to refused cases during his reviews.

16. As regards which panel judge will consider an application, this would be determined by the Judiciary rather than chosen by the LEAs.

17. It may not be practicable to make it a mandatory requirement to make reference to previous applications, since, say, a different LEA or unit may be making subsequent applications. However, we would encourage the LEAs to provide such information to the panel judge when making their applications as far as practicable.

Clause 11 - Application for renewal of judicial authorization

Clause 17 - Application for renewal of executive authorization

If an application for renewal is not made before an authorization ceases to have effect, is there any prohibition against making a fresh application? If not, is there any requirement to refer to previous applications being made?

18. The Bill provides that before an authorization ceases to have effect, LEA officers may apply to the relevant authority for the renewal of the authorization. If after the expiry of an authorization, subsequent developments point to the need to conduct covert operations in respect of the same target covered by a previous authorization, a fresh application

may be made. Please also see paragraph 17 on reference to previous applications.

What would be the arrangements for application for renewal of judicial authorization? Would the same panel judge deal with renewal of application that he has previously approved?

19. The question of which panel judge would consider an application under the Bill, whether a fresh application or an application for renewal, would be decided by the Judiciary. In any case, all the relevant information as set out in Schedule 3 of the Bill would have to be provided.

Clause 23 - Application for confirmation of emergency authorization

Please confirm whether information obtained by carrying out interception or Type 1 surveillance pursuant to an emergency authorization to which no application for confirmation has been made would not be destroyed if it could otherwise be obtained. If not, how would such information be used? Would the same policy apply under Clause 24, 26 and 27?

20. Clause 23(3)(a) provides that if an application for confirmation of emergency authorization is not made, the head of department shall cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or Type 1 surveillance. There is also a similar provision in respect of oral applications (see clause 26(3)(b)).

21. The destruction provisions are included to ensure that information which should have been obtained pursuant to a prescribed authorization should, in a case where the authorization is no longer available, be destroyed. In case, however, any part of the information could have been obtained by other means without an authorization, it would be reasonable not to require its destruction. The provision "to the extent that it could not have been obtained without" is essentially for the avoidance of doubt.

22. As regards instances where applications for confirmation are made

in accordance with the procedures under clause 23 or 26 (in respect of emergency application and oral application respectively), in the event that the relevant authority refuses to confirm the authorization in question, he may make an order under clause 24(3) or 27(3) (as the case may be) for the immediate destruction of any information obtained by carrying out the operation concerned to the extent that the information could not have been obtained without carrying out the operation, or to such an extent as specified in the order. Since the application has been made as provided for in the Bill, it would be more appropriate for the approving authority to decide how best the information obtained should be disposed of.

23. Please see also our response in respect of clauses 26 and 27 in paragraphs 24-26 below.

Clause 26 - Application for confirmation of prescribed authorization or renewal issued or granted upon oral application

Clause 27 - Determination of application for confirmation of prescribed authorization or renewal issued or granted upon oral application

The drafting is not clear if it is the head of department or the relevant authority who would decide the extent to which information would be destroyed under Clause 26 and 27.

24. Clause 26(3)(b) provides that if no application for confirmation is made in 48 hours, "the head of the department concerned shall ... cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or covert surveillance." The extent of the destruction is already prescribed under the provision. In any case, the approving authority would not be involved since no confirmation application is made.

25. Clause 27(3), on the other hand, provides that "[w]here the relevant authority refuses to confirm the prescribed authorization or renewal under subsection (1)(*b*), he may make one or more of the following orders –

(a) .....

(b) in any case whether or not the prescribed authorization or

renewal still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent –

(i) subject to subparagraph (ii), that it could not have been obtained without carrying out the interception or covert surveillance; or

(ii) where paragraph (*a*)(ii) applies, that is specified in the order."

26. In other words, when (a)(ii) applies (i.e. that a variation order is made), the extent would be specified by the panel judge. Otherwise the extent would be that such information could not have been obtained without carrying out the operation in question, as prescribed in the provision.

Clause 29 - What a prescribed authorization may authorize or require

Clause 30 - What a prescribed authorization further authorizes

Why does Clause 29(6) and (7) use "also authorizes"? This is not consistent with the heading of the clause nor does it reflect the policy intent stated in the Explanatory Memorandum. You may note that "further" is used in Clause 30 and its heading.

27. Clause 29(6) and (7) authorizes actions which are essential for carrying out the authorized covert operations, such as the installation and use of devices on the specified object or premises etc. They are dependent upon the operations authorized under subsection (1) to (5) of the clause, and hence what would "also" be authorized here would be consequential upon on what "may" be authorized under the terms of the provision.

Clause 31 - Prescribed authorization may be issued or renewed subject to conditions

Does Clause 31 intend that the relevant authority may specify any condition in a prescribed authorization that would apply to any subsequent authorizations? What is "further authorization or requirement"? If so, can the relevant authority involved in the subsequent application for authorization amend or revoke the condition when issuing further authorization or requirement?

28. Clause 31 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). Thus, "further authorization or requirement" refers to those under the prescribed authorization in question (such as those under clause 29 or 30), and not another prescribed authorization issued subsequently.

Clause 38 - The Commissioner

Is it possible to apply for judicial review of the decision of the Commissioner?

29. As with the decisions of other public offices, the Commissioner's decisions may be subject to judicial review.

Is reappointment also on the recommendation of CJ?

30. It is our intention that CE would reappoint the Commissioner on the recommendation of CJ.

Is it possible that the Commissioner may face a conflict of interest situation in his review or examination? If so, what could be the solution?

31. There are established procedures for dealing with conflicts of interests that may arise in public offices in general, such as by declaring the possible conflict. Given that the Commissioner would be a serving or former senior judge, we trust that he would observe the highest standards to prevent any possible conflict of interest.

Clause 39 - Functions of Commissioner

What other functions are anticipated to be imposed or conferred on the Commissioner under the regulation to be made under Clause 62 and other enactments?

32. The provision under clause 39(b)(iv) and reference to other enactments under clause 39(b)(v) are included to provide for flexibility. There are no other anticipated functions at this stage.

What powers does the Commissioner have in conducting reviews and carrying out examinations? Is it necessary to specify them in the Bill?

33. The powers of the Commissioner for conducting reviews and examinations are provided for under relevant clauses under the respective parts of the Bill, and his further powers (such as requiring officers to answer questions or submit reports) are provided under clause 51.

Clause 43 - Examination by Commissioner

Would the applicant be informed that the Commissioner would not give any notice or make any order? Can the Commissioner give notice or make order when it is no longer prejudicial to the prevention or detection of crime or the protection of public security?

34. Clause 43(5) provides that "(n)otwithstanding subsections (2) and (3), the Commissioner shall not give any notice or make any order under those subsections for ***so long as*** he considers that the giving of the notice or the making of the order (as the case may be) would be prejudicial to the prevention or detection of crime or the protection of public security" (emphasis added). Therefore, when giving notice is no longer considered prejudicial to the matters above, notice may be given. As the Commissioner may not be able to foresee whether he would indeed not give any notice (or make any order) in respect of a case indefinitely, it would be difficult for him to so inform the applicant at the outset.

Clause 47 - Annual reports to Chief Executive by Commissioner

What would be the anticipated circumstances that publication of any matter in the annual report would be prejudicial to the prevention or detection of crime or the protection of public security?

35. We trust that, in all probability, the Commissioner would not include in his report any matter that would be prejudicial to the prevention or detection of crime or the protection of public security. However, in the very unlikely event that such matters are included in the report, it would be in the public interest for them to be excluded. CE would only do so after consulting the Commissioner.

36. It would be impossible to list exhaustively the circumstances where publication of information would be prejudicial to the prevention or detection of crime or the protection of public security.

Clause 58 - Non-admissibility of telecommunications interception product

What is the intention of this Clause? What does it mean by proceedings before any court to prove that a relevant offence has been committed? What kind of offence does the term "relevant offence" include? What does "information that continues to be available for disclosure" mean?

37. The intention of this clause is that product of telecommunications interception is not admissible in proceedings in court in order to, inter alia, minimize the infringement of privacy to the targets and third parties. However, there are offences where the prosecution of which would essentially depend on proving that interception product has been disclosed, for example, those under the Telecommunications Ordinance governing disclosure of intercepted materials. In such cases it would be necessary to admit such materials into court to prove that disclosure was made illegally.

38. Given the policy intention that protected product be destroyed as soon as its retention is no longer necessary for the relevant purpose for which it was obtained, we envisage that in most cases such product would not be available for disclosure. However, to cater for the possibility that the relevant information is still available and its disclosure might be necessary to ensure the fairness of the trial or in the interest of justice, we have included the provision.

Clause 59 - Code of Practice

Is the Code of Practice to be made public and would it be subject to scrutiny of the Legislative Council? Would the Code be ready at the time when the Bill comes into operation?

39. As explained in the paper submitted for information of the Panel on Security on 16 February 2006, the Code of Practice will be made public, but it would not be in the form of subsidiary legislation. Our intention is that the Code of Practice will be in place when the Bill comes into operation.

Clause 61 - Immunity

Please confirm that under Clause 61, there is no immunity for liability for entry on to premises or interference with property without permission. What is the purpose of the phrase "only of"?

40. Clause 61(1) provides for the necessary immunity for carrying out the authorizations or carrying out other acts permitted or required under the Bill. Clause 61(2) further provides that "[n]othing in subsection (1) affects any liability that is or may be incurred by any person by reason only of –

(a) any entry onto any premises without permission; or

(b) any interference with any property without permission."

41. It follows that to the extent that the liability is incurred by reason only of entry onto premises or interference with property without permission, no immunity is to be provided under clause 61(1). The reference to "only of" is necessary in both Clauses 61(1) and 61(2) respectively – the expression restricts the immunity provided under clause 61(1) to those acts only under clause 61(1)(a) to (c) (and not other conduct done in conjunction with such acts), and restricts the "exclusion" from the immunity to the entry onto premises etc. without permission (and not other conduct that would have been involved when unauthorized trespassing is committed).

Clause 65 - Transitional arrangements

What is the policy intent of this Clause?

42. The policy intent of this clause is to apply the proposed safeguards under the new regime on safeguards for materials and admissibility to the products that have been obtained before the Bill takes effect, such that such products would be subject to the same requirements for, for example, retention and destruction as with the newly obtained products under the new regime. Since the same privacy and policy considerations apply, we consider it appropriate to apply the safeguards to pre-existing materials. This would better protect the privacy of the parties concerned.

Schedule 5 - Consequential Amendments

Section 33 of the Telecommunications Ordinance (TO)

What are the reasons for this new section, in particular the power of the Chief Executive to order that any class of messages to be intercepted for the execution of prescribed authorizations?

43. Section 33 of the TO currently reads –

> *"Whenever he considers that the public interest so requires, the Governor, or any public officer authorized in that behalf by the Governor either generally or for any particular occasion, may order that any message or any class of messages brought for transmission by telecommunication shall not be transmitted or that any message or any class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order".*

Under this section, the CE may, when he considers it to be in the public interest, order the interception of telecommunication messages, including both what is normally understood to be the "contents" and the "non-contents" parts of the messages. In the judgment of the Court of First Instance in February 2006 on the constitutionality of the section, the court declared that **insofar as that provision authorizes or allows access to or disclosure of the contents of any message**, it is unconstitutional.

44. In line with the judgment of the Court of First Instance on the constitutionality of the provision, which has not been a subject of further appeal, we have proposed to amend section 33 of the TO as currently provided for under clause 5 under Schedule 5 of the Bill. The amended section 33 of the TO seeks to preserve that part of the provision that has not been ruled unconstitutional by the court. This is required to enable, for example, the Office of the Telecommunications Authority (OFTA) to undertake its investigations into contraventions by unlicensed operators of international calls under the Telecommunications Ordinance, as well as to allow the execution of prescribed authorizations when they are issued, i.e., the interception of "non-contents" parts of the messages in question.

45. We have taken the opportunity to provide safeguards in the amended provision. First, instead of relying on the usual meaning of "contents", i.e., the communication part of a message, we have borrowed the same broad meaning of "contents" as in the Bill, i.e., "the contents of any communication transmitted by a telecommunications system include <u>any data</u> produced in association with the communication" (emphasis added). Then the revised section 33(2) makes it clear that an order shall not of itself authorize the obtaining of contents of any individual message. Hence, the order to be made by CE under this revised provision cannot authorize the obtaining of <u>any data</u> (voice and other data) in association with any individual message. There would be no interference with any privacy of communication.

46. Further, the revised provision stipulates that no data about any individual message may be <u>obtained</u> (revised section 33(2)). There is therefore no question of the messages being recorded and <u>stored</u> by way of the order. As there would be no interference with the privacy of communications, it is appropriate for CE to be the authorizing authority.

Section 58A of the Personal Data (Privacy) Ordinance

Please clarify why section 57 (personal data held for the purposes of safeguarding security, defence or international relations) and 58 (personal data for the purposes of the prevention or detection of crime) of the Personal Data (Privacy) Ordinance would not duplicate the new section 58A.

47. The coverage of section 58A would be wider than that under

sections 57 and 58 – personal data in protected products or relevant records (i.e. applications and the authorization / warrants themselves) may be itself held for the purpose of safeguarding security, or prevention and detection of crime, etc. However, such records are an essential part of the regime under the Bill. To avoid overlapping of the purview of the Commissioner under our Bill and the Privacy Commissioner for Personal Data, the new section 58A is proposed.

Section 17 of the Official Secrets Ordinance

Why does the amendment cover only interception product and not surveillance product?

48. The amendment will be a consequential one. The present section 17 of the Official Secrets Ordinance (OSO) is applicable to information from interception obtained under section 33 of the Telecommunications Ordinance and section 13 of the Post Office Ordinance. The amendment proposed under the Bill to the OSO corresponds to the existing scope of the provision. This extra protection is in line with our general approach towards this more intrusive mode of covert operation.

Security Bureau
April 2006