For information
25 March 2006 **SB Ref: ICSB 2/06**

Bills Committee on
Interception of Communications and Surveillance Bill

Response to issues raised by Members
at the meeting of 16 March 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Bills Committee on 16 March 2006.

Response to issues raised

Issue 1 : To provide information on the definition of "public security" in other jurisdictions.

2. Clause 3 of the Bill sets out the conditions for issue, renewal or continuance of a prescribed authorization for interception of communications or covert surveillance. Among other things, the purpose of the proposed authorization has to be either of the following –

(a) preventing or detecting serious crime; or

(b) protecting public security.

This follows closely the wording of Article 30 of the Basic Law, which reads –

> "…the relevant authorities may inspect communication in accordance with legal procedures *to meet the needs of public security* or of investigation into criminal offences" (emphasis added).

3. The Bill does not define the term "public security". This approach is consistent with that adopted in the 1996 Law Reform Commission report on interception of communications, the 1997 White Bill on Interception of Communications and the 1997 Interception of Communications Ordinance.

4. Security protection is a usual ground for authorizing interception of communications and covert surveillance by the law enforcement agencies in other jurisdictions. For the five jurisdictions the legislation of which we have taken into account in drawing up our legislative proposals (i.e., the United Kingdom (UK), Australia, the United States (US), Canada and New Zealand), the situation is as follows –

- UK : Under the Regulation of Investigatory Powers Act (RIPA) 2000, an interception warrant or an authorization for covert surveillance may be issued or granted if the warrant or authorization is necessary, inter alia, "in the interests of national security".

- Australia : Obtaining intelligence relating to "security" is a ground for carrying out interception of communications under the Telecommunications (Interception) Act (TIA) 1979 and covert surveillance under the Australian Security Intelligence Organisation Act (ASIOA) 1979.

- US : Acquisition of "foreign intelligence information" is one of the grounds for conducting "electronic surveillance" under the Foreign Intelligence Surveillance Act (FISA). "Foreign intelligence information" is defined as including "information with respect to a foreign power or foreign territory that relates to ... the national defense or the security of the United States".

- Canada : Investigation into "a threat to the security of Canada" is one of the grounds for conducting interception of communications or "obtain[ing] any information, record, document or thing" under the Canadian Security Intelligence Service Act (CSISA).

- New Zealand : "Detection of activities prejudicial to security" and "gathering [of] foreign intelligence information essential to security" are grounds to "intercept or seize any communication, document, or thing" under the New Zealand Security Intelligence Service Act (NZSISA) 1969. The protection or advancement of the "security" of New Zealand is also a ground to intercept communications with an interception device under the Government Communications Security Bureau Act (GCSBA) 2003.

5. The practice as to whether terms like "security" or "national security" are defined in the respective legislation varies –

- UK : The RIPA does not provide for a definition of the term "national security".
- Australia : The TIA follows the same definition as "security" as in the ASIOA. The latter definition is reproduced at **Annex A1**.
- US : "Security" is not defined in the FISA.
- Canada : The definition of "threats to the security of Canada" is provided for in the CSISA, reproduced at **Annex A2**.
- New Zealand : The definition of "security" is provided for in the NZSISA (but not GCSBA), reproduced at **Annex A3**.

6. In summary, while all five jurisdictions allow covert operations on the ground of security, only three of them provide a statutory definition of the concept. Where terms like "security" or "national security" are defined in legislation providing for interception of communications and covert surveillance, the definitions tend to be broad. More generally, the jurisprudence in this area also indicates that a legal definition of the term is not a necessity. In the *Esbester*[1] case, the European Commission of Human Rights stated that the term "national security" is not amenable to exhaustive definition. The Bill's current approach of not defining the term "public security" is consistent with the approach taken in previous discussions on the subject, taking into account the general difficulty to list out exhaustively the circumstances under which public security would be threatened in legislative terms.

7. We must reiterate that the purpose is only one of the first hurdles in obtaining authorizations for interception and covert surveillance operations. The approving authority needs to be satisfied that the tests regarding proportionality and necessity are met before an authorization for interception of communications or covert surveillance may be granted. Also, operations conducted under the Bill would be

---

[1] *Esbester v United Kingdom* (1993) 18 EHRR CD 72.

subject to other safeguards in our proposed regime.

Issue 2 : To explain the exceptions to the protection of legal professional privilege and the effect of Article 35 of the Basic Law, and to provide the Administration's response to the views given by the judge in the English case of Three Rivers District Council and Others v Governor and Company of the Bank of England .

8. Communications between a client and his legal advisor, whether oral or in writing, are privileged from disclosure, **IF –**

- those communications are for the purpose of obtaining legal advice, whether or not legal proceedings are in train,
- except when such communications are in furtherance of a criminal purpose .

In connection with the latter point, the courts of Hong Kong, like their counterparts in England, have made it abundantly clear that communications in furtherance of a criminal purpose are not protected by the privilege.

9. This principle of legal professional privilege (LPP) is firmly established under the common law. There can be no exceptions to this privilege, unless the client waives it, or it is expressly overridden by statute. Because LPP covers communications for the purpose of obtaining legal advice, it does not apply to other communications between a lawyer and his client. For example, communications between a lawyer and his client on social occasions not for the purpose of obtaining legal advice would in principle not attract LPP. Communications between a lawyer and persons who are not his clients are not covered by LPP.

10. More details of LPP and the effect of Article 35 of the Basic Law, and the Administration's response to the views given by the court in the case of *Three Rivers District Council and Others v Governor and Company of the Bank of England*, are at **Annex B**. In drafting our Bill, we have set out to protect LPP, as follows.

11. Under our Bill, interception of communications and more intrusive (Type 1) covert surveillance operations would be considered by judges. For less intrusive (Type 2) covert surveillance operations, our

general regime is for them to be approved executively. However, as a protection of LPP, we propose that in cases that may involve LPP, the applications should be considered by judges. Clause 2(3) now reads –

> "For the purpose 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."

Our judges can be expected to be conscious of the principles governing LPP.

Issue 3 : To explain the difference between "confidential information" and "highly sensitive information" referred to in the paper "Proposed Integrity Checking on Panel Judges" (LC Paper No. CB(2)1423/05-06(03)).

12. In its paper CB(2)1423/05-06(03), the Judiciary has pointed out that –

(a) normally judicial officers are subject to appointment checking prior to their appointment; and

(b) the Chief Justice (CJ) and Permanent Judges of the Court of Final Appeal (CFA) are subject to normal checking The rationale is that the position of CJ, as the head of the Judiciary, involves regular access to information classified as confidential; and Permanent Judges of the CFA may act as CJ in the latter's absence.

As far as the CJ position is concerned, the Judiciary has advised that the types of confidential information to which CJ has access on a regular basis include communications with the Administration concerning : (i) the preparation of Executive Council memoranda relating to the administration of justice or otherwise impacting on the operation of the Judiciary; (ii) the Administration's policy and/or legislative proposals relating to such matters; and (iii) preparation of the Judiciary's annual draft estimates of expenditure, which forms part of the Administration's overall budget.

13. The above arrangement is in line with the basic principles for

deciding on the need for and types of checking required for other positions. We have set out these principles in the paper presented to the Panel on Security for discussion on 7 March 2006 (relevant extracts at **Annex C**). Essentially, the particular circumstances of individual cases, taking into account, among other things, the level and type of information to which the prospective appointee may have access to, and the frequency with which he may have access to such information, determine the appropriate type of checking required. The main criterion for assessing the classification of information/documents is the degree of damage unauthorized disclosure of the material in question or its source would cause.

14. Viewed collectively, the types of information to which panel judges to be appointed under the Bill would have extensive and regular access are more sensitive than the confidential information that CJ in his capacity as head of the Judiciary has access to. The key difference is the wide range of cases that have to be kept covert for a long time or even indefinitely in interception of communications and covert surveillance cases. In some instances, the unauthorized disclosure of the information involved could reveal the identities of key informants, put witnesses or law enforcement officers at serious physical risk or even risk of death, ruin years of investigation or significantly damage our cooperation with LEAs in other jurisdictions. (Some examples of real cases illustrating the sensitive nature of the information and the operations involved are at **Annex D**.) Taken as a whole, therefore, the information involved should be subject to the highest level of protection.

15. In addition, the range and types of sensitive information to which panel judges would have access under the Bill are not the same as those considered in general court proceedings. On this, the relevant extracts of previous papers submitted to the Panel of Security and the Bills Committee (SB Ref: ICSB 01/06) are at **Annex E**.

16. In conclusion, it is noteworthy that the existing arrangements for checking judges as set out in paragraph 12 above –

(a) are in line with the Government's standard arrangement for protecting sensitive information;

(b) do not indicate in any way a lack of trust in the CJ and the Permanent Judges of the CFA, in general or in relation to the

confidential information they may have access to;

(c) do not involve any political assessment; and

(d) have not affected and will not affect the independence of the CJ and the Permanent Judges in any way, nor the independence of the Judiciary as a whole.

The same applies to our plan for subjecting the panel of three to six judges to extended checking, on par with their supporting staff, the proposed Commissioner on Interception of Communications and Surveillance (the Commissioner) and his staff, and existing LEA officers with similar access to sensitive information.

Issue 4: To explain whether an authorization given by a panel judge for interception of communications or surveillance is a judicial authorization.

17. Under the Bill, there would be a self-contained authorization regime for granting authorizations by judges. The Bill expressly provides that in exercising their powers a panel judge shall act judicially and have the same powers and immunities as a judge of the Court of First Instance. The need for this arrangement and its difference from other cases considered by the court are set out in the extracts of previous papers submitted to the Panel on Security and the Bills Committee (SB Ref: ICSB 01/06) at **Annex E**.

18. At the same time, the sensitive and covert nature of applications for interception of communications and Type 1 surveillance necessarily makes the normal rules attendant on court proceedings (e.g. rules governing legal representation, disclosure and appeal) not applicable to the consideration of such applications. Schedule 2 of the Bill thus sets out the procedures and other matters relating to the panel judges. Clause 4 of the Schedule provides that –

> "In performing any of his functions under this Ordinance, a panel judge shall act judicially and have the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court."

19. By providing that they will have the same powers, protection

and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court when performing their functions as panel judges, the Bill further underlines their independence in exercising their judicial functions. It is therefore appropriate that the authorizations are referred to as judicial authorizations.

20. The position of the panel judges may also be contrasted with that of the Commissioner, who would operate away from the Judiciary in carrying out his functions under the Bill. Indeed, under the Bill, the Commissioner, although a former or sitting judge, is not required to act judicially in carrying out his review functions. In this regard, the Commissioner's position would be more akin to that of a judge appointed to perform a non-judicial function, e.g., as the chairman of the Electoral Affairs Commission.

21. Under the Bill, the panel judges would have to be serving judges of the Court of First Instance, and would continue to be part of the Judiciary in carrying out their functions. The Judiciary confirms that this arrangement is acceptable. The Administration and the Judiciary are now discussing the detailed arrangements regarding the application procedures governing judicial authorizations against this backdrop.

Security Bureau
March 2006

Annex A1

Definition of "security" in Australian legislation

Australian Security Intelligence Organisation Act 1979

"Security " is defined under section 4 of the Act as follows -

"(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a). "

Annex A2

Definition of "threat to the security of Canada" in Canadian legislation

Canadian Security Intelligence Service Act (Chapter C-23)

The Act allows the granting of a warrant to enable the Security Service to investigate "a threat to the security of Canada". Section 2 of the Act defines "threats to the security of Canada" as meaning:

> "(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
>
> (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,
>
> but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d)."

Annex A3

Definition of "security" in New Zealand legislation

New Zealand Security Intelligence Service Act 1969

Section 2 of the Act (as amended)[1] defines "security" as follows:

"(a) The protection of New Zealand from acts of espionage, sabotage, terrorism, and subversion, whether or not they are directed from or intended to be committed within New Zealand;

(b) The identification of foreign capabilities, intentions, or activities within or relating to New Zealand that impact on New Zealand's international well-being or economic well-being;

(c) The protection of New Zealand from activities within or relating to New Zealand that -

(i) Are influenced by any foreign organisation or any foreign person; and

(ii) Are clandestine or deceptive, or threaten the safety of any person; and

(iii) Impact adversely on New Zealand's international well-being or economic well-being;

(d) the prevention of any terrorist act and of any activity relating to the carrying out or facilitating of any terrorist act."

---

[1] See New Zealand Security Intelligence Service Amendment Act (No. 2) 1999 and New Zealand Security Intelligence Service Amendment Act 2003.

Annex B

Interception of Communications and Covert Surveillance

Legal professional privilege

At the Bills Committee meeting on 16 March 2005, Hon Alan Leong SC referred to the judgment of Lord Scott in *Three Rivers District Council v Governor and Company of the Bank of England* [2005] AC 610 at paragraph 25 to support the view that legal professional privilege ("LPP") is absolute. The relevant paragraphs read:

> *"[24] First, legal advice privilege arises out of a relationship of confidence between lawyer and client. Unless the communication or document for which privilege is sought is a confidential one, there can be no question of legal advice privilege arising. The confidential character of the communication or document is not by itself enough to enable privilege to be claimed but is an essential requirement.*
>
> *[25] Second, if a communication or document qualifies for legal professional privilege, the privilege is absolute. It cannot be overridden by some supposedly greater public interest. It can be waived by the person, the client, entitled to it and it can be overridden by statute ... , but it is otherwise absolute. There is no balancing exercise that has to be carried out ... . The Supreme Court of Canada has held that legal professional privilege although of great importance is not absolute and can be set aside if a sufficiently compelling public interest for doing so, such as public safety, can be shown ... . But no other common law jurisdiction has, so far as I am aware, developed the law of privilege in this way. Certainly in this country legal professional privilege, if it is attracted by a particular communication between lawyer and client or attaches to a particular document, cannot be set aside on the ground that some other higher public interest requires that to be done."*

2. The common law has long recognised that the right to confidential legal advice is of such importance to the due administration of justice that justice itself is undermined if that right is compromised. As Lord Taylor CJ expressed it in *R v Derby Magistrates Court, ex parte B* [1996] 1 AC 487: *"[LPP] is a fundamental condition on which the*

administration of justice as a whole rests. ... I am of the opinion that no exception should be allowed to the absolute nature of legal professional privilege, once established."

3. The purpose of LPP is to enable a client to make full disclosure to his legal adviser for the purposes of seeking legal advice without apprehension that anything said by him in seeking advice or to him in giving it may thereafter be subject to disclosure against his will. Lord Bingham CJ pointed out in *R v Manchester Crown Court, ex parte Rogers* [1999] 1 WLR 832 that *"legal professional privilege applies, and applies only, to communications made for the purpose of seeking and receiving legal advice."*

4. In a similar vein, Lord Bingham CJ stated in *Paragon Finance plc v Freshfields* [1999] 1 WLR 1183 that: *"Save where client and legal adviser have abused their confidential relationship to facilitate crime or fraud, the protection is absolute unless the client (whose privilege it is) waives it, whether expressly or impliedly."*

5. Irrespective of whether LPP is absolute or not, LPP will not apply in respect of communications made in order to obtain advice for a criminal purpose. This exception applies whether the lawyer knows or is ignorant of the criminal purpose: *Pang Yiu Hung Robert v Commissioner of Police*, HCAL 133/2002, para 24.

6. LPP is also protected by the Basic Law and the International Covenant for Civil and Political Rights ("the ICCPR"). Article 35 of the Basic Law guarantees that: *"Hong Kong residents shall have the right to confidential legal advice, access to the courts, choice of lawyers for timely protection of their lawful rights and interests or for representation in the courts, and to judicial remedies. ..."*

7. The common law rule on LPP is therefore expressly entrenched in the Basic Law and has a protected status. Although a number of cases have referred to the right to confidential legal advice under Article 35 of the Basic Law,[1] none of them have explained the scope of this right or commented on the difference between the constitutional right and the rule protecting privileged communications from disclosure at common law.

---

[1] Eg, *Pang Yiu Hung Robert v Commissioner of Police* HCAL 133/2002, 2 December 2002 (CFI); *A Solicitor v Law Society of Hong Kong*, CACV 246/2004, 9 June 2005, (CA); *Secretary for Justice v Shum Chiu*, HCAL 101/2005, 22 December 2005, (CFI)

8. Article 87 of the Basic Law is also relevant. It provides that: *"In criminal or civil proceedings in the Hong Kong Special Administrative Region, the principles previously applied in Hong Kong and the rights previously enjoyed by parties to proceedings shall be maintained. ..."* This Article makes it plain that LPP, as a right enshrined in the common law and fashioned by the common law prior to the change of sovereignty, has remained of equal force and effect after it.[2] However, the Court in *Pang v Commissioner of Police* also said (at para 23): "*With regard being had to any constitutional restraints, it is accepted that LPP may be limited by legislation. This will be so when there is express statutory language to that effect or when, as a matter of interpretation, the implication that it is limited is clearly necessary."*

9. Article 39(1) of the Basic Law also provides that the provisions of the ICCPR as applied to Hong Kong shall remain in force and shall be implemented through the laws of the HKSAR. By virtue of Article 14(3)(b) of the ICCPR, an accused person must have adequate time and facilities for the preparation of his defence and "to communicate with counsel of his own choosing". According to the UN Human Rights Committee, this subparagraph requires counsel to communicate with the accused in conditions giving full respect for the confidentiality of their communications.

10. Article 39(2) of the Basic Law provides that any restrictions on the rights and freedoms enjoyed by Hong Kong residents must be prescribed by law and be consistent with the provisions of the ICCPR as applied to Hong Kong. The rights and freedoms enjoyed by Hong Kong residents may be provided for (a) in both the Basic Law and the ICCPR; or (b) only in the Basic Law and not in the ICCPR; or (c) only in the ICCPR but not in the Basic Law: *Bahadur v Director of Immigration*, FACV 17/2001 (30 July 2002), para 26. As far as the right to confidential legal advice is concerned, it is provided for in both the Basic Law and the ICCPR.

11. In *New World Development Co Ltd v Stock Exchange of Hong Kong Ltd* CACV 170/2004, at para 156, Reyes and Yeung JJA held, in the context of the right to legal representation under Article 35 of the Basic Law, that: "*A right under art. 35 is not absolute. It may be restricted for good reason, provided the restriction imposed is*

---

[2] *Pang Yiu Hung Robert v Commissioner of Police* HCAL 133/2002, 2 December 2002, at para 18; and *Secretary for Justice v Shum Chiu*, HCAL 101/2005, 22 December 2005, at para 17.

proportionate to the reason and does not have the effect of negating the right."

12. In *Ng Yat Chi v Max Share Ltd*, FACV 5/2004, para 73, the Court of Final Appeal held, in the context of the right of access to the courts under Article 35 of the Basic Law, that: *"In relation to BL 35 and BOR 10, it has firmly been established in the jurisprudence of the European Court of Human Rights in relation to the closely analogous right of access under Art 6(1) of the European Human Rights Convention, that such right is by its nature not absolute, but may be subject to limitations. Such limitations are valid if they pursue a legitimate aim, are proportionate to that aim and are not such as to impair the very essence of the right".*

13. The expression "items subject to legal privilege" is defined in section 2(1) of the Organized and Serious Crimes Ordinance (Cap 455) as meaning:

> "*(a) communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;*
>
> *(b) communications between a professional legal adviser and his client or any person representing his client or between such an adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings; and*
>
> *(c) items enclosed with or referred to in such communications and made-*
>
> *(i) in connection with the giving of legal advice; or*
>
> *(ii) in connection with or in contemplation of legal proceedings and for the purposes of such proceedings,*
>
> *when they are in the possession of a person who is entitled to possession of them,*
>
> *but excludes any such communications or items held with the intention of furthering a criminal purpose".*

14. The United Nations (Anti-Terrorism Measures) Ordinance (Cap 575), the Mutual Legal Assistance in Criminal Matters Ordinance

(Cap 525), and the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap 405) also adopt this definition.

15. Hartmann J explained in *Pang v Commissioner of Police* (at para 43) that the intention of the legislature is to encapsulate the common law principles governing LPP including the exception to the privilege, and referred to the exception to legal privilege established in *R v Cox and Railton*, 14 QBD 153, which provides that no legal privilege attaches to legal advice obtained for the purpose of committing crime. He added (at paras 120 to 122) that: "*if LPP is an absolute right then (as with absolute privilege in judicial proceedings) it is a privilege to be kept within defined boundaries and courts should be slow to extend the scope of the privilege ... . The law, of course, has always recognised that LPP has its limits and those limits are to a material extent defined by the vulnerability of LPP to exploitation and abuse. As Lord Justice Parker said in Banque Keyser Ullmann v. Skandia (UK) Insurance (supra) 'it would be monstrous for the Court to afford protection ... in respect of communications which are made for the purpose of fraud or crime.'*"

16. As to when LPP does or does not apply, Hartmann J said (at para 128) that "*lawyers have always been obliged to understand its limits and to act accordingly. Clients too should know that it has its limits and is not, by means of disguising their true intent from their lawyers, an invulnerable mechanism for seeking advice on (or being helped in) the pursuit of criminal purposes.*"

17. In *Secretary for Justice v Shum Chiu*, HCAL 101/2005, at paras 30 to 32, the Court noted that:

> "*not all meetings between client and professional legal adviser are privileged. The privilege applies only to communications made bona fide for the purpose of seeking and receiving legal advice. If the communications are made in order to obtain advice for a criminal purpose then, of course, legal professional privilege does not attach itself to those communications. This exception applies whether the lawyer is a knowing party or is ignorant of the criminal purpose and is being used as an innocent tool by the client alone and/or with third parties to advance a criminal purpose. … That being the case, it must follow, I think, that if there are objectively cogent grounds for believing that a meeting, which prima facie is protected by legal professional privilege, is in fact to be used in order to*

> *further a criminal enterprise – and will not therefore in fact be privileged – then the investigating authorities must be able to discover what has passed at that meeting."*

18. In *A Solicitor v Law Society of Hong Kong*, CACV 246/2004, the Court of Appeal stated (at para 14) that *"it is unquestionable that legal professional privilege is absolute and is based not merely upon the general right to privacy but also the right of access to justice"*. However, in determining whether section 8B (document production and privilege) of the Legal Practitioners Ordinance (Cap 159) contravened the Basic Law, the Court also held (at paras 15 to 16) that:

> "*Legal professional privilege has always been subject to the principle that it is subject to the public policy that the privilege will not extend to transactions in furtherance of crime or fraud. … If legal professional privilege could be prayed in aid to prevent investigations other than those sanctioned by lay clients, the investigation by the Law Society of complaints against solicitors would be hamstrung. Therefore, the insertion into the Ordinance of a provision which allows investigations is clearly in the public interest provided that there are adequate safeguards which makes the relaxation of the fundamental rule proportional."*

Department of Justice
March 2006

Annex C

Interception of Communications and Covert Surveillance

Relevant Extracts from the Information Paper for the meeting of LegCo Panel on Security titled "Pre-Appointment Checking"

7. It is a long-standing and standard arrangement for checks to be conducted to ascertain the risks, if any, that might be involved in the appointment of an individual to a certain position. It is a routine procedure for various Government appointments, including appointments to civil service posts and to certain advisory and statutory bodies. The need for and types of checking required will depend on the particular circumstances of each individual case and take into account, among other things, the level and type of information to which the prospective appointee may have access and other relevant factors such as the frequency with which he may have access to such information, and the degree of control he may have over such information. Given its nature, the checking is normally done at the end of the appointment process when the candidate is considered suitable in all other respects.

8. As pointed out at the Security Panel meeting on 2 March 2006, the subject of "Integrity Checking for Disciplined Forces" has been the subject of discussion of the Panel on Security. Copies of the relevant papers submitted by the Administration for the May 2004 Panel meeting on the subject are at **Annex A**. In response to the concerns of Members regarding the related issue of checking of persons to be appointed to advisory and statutory bodies, to be Justices of the Peace and Principal Officials, upon the request of Members, supplementary information was subsequently provided to Members (a copy of the subsequent information paper is at **Annex B**).

not attached

not attached

9. As can be seen from the Annexes, broadly speaking there are three levels of checking : appointment checking, normal checking and extended checking, with the last one being the most extensive. Extended checking is applicable to all people to be appointed to the most senior positions in the Government, e.g., Principal Officials and senior civil servants. It is also applicable to those who have access to very sensitive information. This is the checking that we have been doing for law enforcement officers with wide access to the more sensitive

information arising from covert operations and will do for panel judges, the oversight authority, and their staff.

10. In extended checking, the prospective appointee will be requested to provide information on his personal particulars, educational background, social activities, employment history and family members. He will also be asked to nominate two referees. The checking will comprise interviews with the prospective appointee, his referees and supervisors as well as record checks. The checking is therefore much more thorough in order to help the appointment authority assess if there is any possible risk in appointing a candidate to a position involving much sensitive information. It **does not involve** any form of political vetting, and no investigation will be conducted on the political beliefs or affiliations of a prospective appointee.

11. Extended checking does not focus only on the "integrity" per se of the prospective appointee. There may well be factors unrelated to a person's personal "integrity" and beyond their control (for example, association of family members), that may expose them to a greater risk of, say, possible conflict of interests, than would otherwise be the case. In the case of the panel judges under discussion, there should not be doubts about their "integrity", but it is not inconceivable that a person is suitable to be a judge but circumstances are such that, without any reflection on his "integrity", it would not be appropriate for him to sit or continue to sit on the panel. Partly for this reason, and as mentioned in our previous papers, the Bill provides for CE to revoke the appointment of a panel judge on the Chief Justice's recommendation and for good cause.

* * * * * * *

Annex D

Interception of Communications and Covert Surveillance

Extract of the affirmation made by the Administration to the Court of First Instance on 26 November 2005 on the Judicial Review Case on Interception of Communications and Covert Surveillance

* * * * * *

Illustrative cases on the use of covert investigation techniques

Arrest of suspected terrorists for extradition to the United States (US)

12. In order to illustrate the importance of use of covert surveillance in criminal investigation, the Police have provided me with some cases where covert surveillance were used to detect crimes. I am informed by the Police and verily believe to be true that in August 2002, the Federal Bureau of Investigation (FBI) requested the Police to provide assistance in its operation after receipt of information that two Pakistanis and an Indian (a naturalized US citizen) would arrange smuggling of a substantial amount of heroin and cannabis from Pakistan to the US, and that they would have meetings with two undercover FBI agents in Hong Kong.

13. The deal was to trade half a tonne of heroin and 5 tonnes of hashish for 4 Stinger anti-aircraft missiles and cash. The missiles were to be sold to the Taliban and Al Qaeda to shoot down American planes.

14. The Police mounted surveillance operations against the Pakistani and Indian males. Such operations were required to cover the meetings between the agents and the suspects, and provide protection to the agents. As a result of the operations, sufficient evidence was obtained to prove their drug activities.

15. Subsequently the Pakistani and Indian males were arrested by the Police and were extradited to the US. One of the two Pakistanis and the Indian pleaded guilty to conspiring to distribute drugs and to provide material support to a foreign terrorist organization.

Shatin Racecourse Bombing

16. I am informed by the Police and verily believe that on 13 June 2002, a suspicious package was found at Level 4 of the grandstand at the Shatin Racecourse. Bomb disposal officers of the Police confirmed that it was an improvised explosive device with a remote control in the form of a mobile phone. The device contained approximately 100 grams of low explosive composition mixed with nails as shrapnel. Investigations identified a suspect, but had yet to unearth evidence to implicate him. The suspect was then placed under covert surveillance. On 17 June 2002, by means of covert surveillance, the Police found that the suspect dropped a plastic bag. Having retrieved the bag, the Police found it to contain paraphernalia for making improvised explosive device. The suspect was immediately arrested and subsequently convicted.

17. Without the use of covert surveillance, it would be impossible to retrieve such significant evidence leading to the swift detection of the case.

Acceptance of illegal commission by a company consultant

18. I am informed by the ICAC and verily believe that there is a case where a company consultant was convicted of accepting over half a million dollars in illegal commission, crucial evidence obtained through the use of covert surveillance was admitted in evidence against the defendant. Before the witness came to the ICAC to report the case, he covertly taped the conversation he had with the defendant in which the latter made a corrupt solicitation. At a subsequent meeting between the defendant and the witness which was covertly monitored by ICAC officers, the witness handed over half a million dollars to the defendant who, after realizing that ICAC officers were after him at the scene, ran away with the bribe money. After a brief chase, the defendant was eventually intercepted inside a toilet nearby and arrested. Recording was also made of what had happened in the ambush operation and prior telephone conversations between the defendant and the witness. In convicting the defendant, the trial judge considered the monitored conversation between the witness and the defendant '*a very important*

piece of evidence' to corroborate the witness. The defendant was given a custodial sentence after trial. Other than the count for which the defendant was convicted, there were in fact seven other similar counts against him in relation to corrupt transactions which took place prior to the complaint being made to the ICAC. As the trial judge found no corroborative evidence like the covert surveillance evidence admitted in respect of the convicted count, he acquitted the defendant on those other charges.

* * * * * *

Annex E

(Annex A3 to Paper SB Ref: ICSB 1/06)

Interception of Communications and Covert Surveillance

Need for a Panel of Judges

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 4: To explain the consideration factors or criteria adopted for proposing the appointment of a panel of judges by the Chief Executive for authorizing interception of communications and the more intrusive covert surveillance operations, and the differences between the aforementioned proposed framework and the framework for authorizing the issuance of search warrants by judges in terms of the role of judges, the procedures involved and the appeal or judicial review of the decisions of judges.

Item 5 : To explain why the Administration considers it appropriate for the Chief Executive to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance, and to clarify the functions of the panel judges, whether the decisions of the panel judges are subject to judicial review and whether the panel judges are subject to any rules or procedures of the court.

18. As regards the framework of the new regime, the Bill provides that a panel judge when carrying out his functions will act judicially, but not as a court or as a member of a court and that he will have all the powers and immunities of a judge of the High Court[2]. Conceptually this is not an unusual arrangement. For example, a Commissioner appointed under the Commissions of Inquiry Ordinance (Cap 86) will similarly not act as a court, although for all intents and purposes he will act judicially in carrying out his functions. Since a panel judge will not be acting as a court, he may be liable to judicial review in respect of his decisions. The Bill seeks to establish a self-contained statutory regime. In this

---

[2] In the case of *Bruno Grollo v. Michael John Palmer, Commissioner of the Australian Federal Police and Others F.C.95/032*, the Australian Court was of the view that issuing an interception warrant was a non-judicial power and as such held that a non-judicial function could not be conferred on a Judge without his or her consent.

respect the proceedings will not be generally subject to rights of appeal or other provisions of the High Court Ordinance or High Court Rules. The similarity with the issue of a subpoena or search warrant is only limited, in that the importance of the issues to be dealt with and their sensitivity are considerably different, hence justifying the setting up of the self-contained statutory regime that we have proposed.

Relevant extracts of Information Paper titled "Panel of Judges" for the meeting of LegCo Panel on Security on 7 March 2006

Need for self-contained regime

4. The Bill sets out a self-contained regime for granting judicial authorizations to cater for the sensitive and covert nature of interception of communications and covert surveillance. The regime is described in the papers that the Administration has prepared for discussion by Members on 7 and 16 February and 2 March 2006. The relevant extracts are at the **Annex** for Members' ease of reference.

not attached

5. At the meeting of the Panel of Security on 2 March 2006, some Members drew a comparison between the consideration of applications for authorization for interception of communications and covert surveillance by the panel of judges on the one hand, with the consideration of claims for public interest immunity (PII) and applications under various ordinances on the other, and asked if the judges would be exposed to the same level of sensitive information in both. We consider that the two are quite different.

6. At the outset, PII is only claimed in very limited circumstances during the course of proceedings which are already before the court. The classes of document or information for which PII has been claimed has included, for example, the identity of undercover police officers or informers, details of how surveillance operations have been carried out in a particular case, other details of law enforcement investigations, memoranda or minutes of meetings of the Executive Council and confidential financial advice. Although the judge may examine the documents or information to determine their relevance to the case, the prosecution, in a criminal case, or the Government as a party to civil proceedings, has the option of dropping the case or making admissions of

fact, if the disclosure of the information would be extremely damaging to public interest or place a person in grave personal danger. Since 1992, when records began, only 27 PII certificates have been issued by the Chief Secretary.

7. Applications under the Organized and Serious Crime Ordinance (OSCO) relate to the production of materials, confiscation of proceeds of crime and search and seizures connected with organized and serious crime. Those under the United Nations (Anti-Terrorism Measures) Ordinance (UN(ATM)O) relate to specification and forfeiture of terrorist property[1]. The applications relate to one-off events, such as requesting an otherwise willing third party (e.g., a bank) who might otherwise be prevented from confidentiality requirements from providing readily available information, in much less covert circumstances (please also see paragraph 12 below).

8. As regards Part XII of the Interpretation and General Clauses Ordinance (IGCO), it relates to the production and search and seizure of journalistic material. Since the enactment of Part XII of IGCO in 1995, only three ex parte applications for warrants have been made.

9. Given that interception of communications and covert surveillance are indispensable investigation tools, the number of cases is necessarily much larger than, say, PII claims. We envisage the number of applications requiring judicial authorizations for these covert operations to be in the hundreds per year. The frequency and level of exposure of the panel judges to sensitive materials would be considerably higher as a result.

10. Another difference is the **identities of the parties**. A PII claim is made in the context of proceedings which have already started. Thus the judge will know the identities of all the parties, and will have an opportunity to consider on a case by case basis if the circumstances of the case require that he recuse himself from the case. Under the Bill, on the other hand, a panel judge will have no prior warning of the subject matter of an application, and will only discover the identity of the target (if

---

[1] The relevant sections have yet to come into effect.

known) when the application is made, by which time the security of the operation and of the material produced in support of the application might have been compromised.

11. Similarly, in OSCO and other ex parte applications to the court, the identities of the target is necessarily known. This is not always the case with interception of communications and covert surveillance operations — the identities of the target may in fact not always be known from the outset. For example, in a drug trafficking case, the identities of some of those involved may not be known at the beginning of the operation. Thus in such cases it would be far less practicable to deal with the sensitivity aspects on a case by case basis. Rather, we should seek to ensure that the system is designed to minimize any confidentiality risks at the outset.

12. The key difference between interception of communications and covert surveillance and other cases is that the former operations will **remain covert** and unknown to the target, and in many cases have to be kept confidential for a long time and sometimes indefinitely to, among other things, protect the identity or safety of personnel involved or ensure continued cooperation with other law enforcement agencies. With PII and other applications, the reverse is true – the operations either have become overt already or will become so almost immediately afterwards. In the case of claiming PII, there is an on-going trial and the question only turns on whether some information should be made available to the defence and / or the public. With respect to the application for a production order for journalistic material under IGCO, the application is made inter partes. In other cases, the operation will turn overt when the authorization is executed. The confidentiality and sensitivity concerns are therefore considerably less. Also, a range of judicial remedies such as appeals to the court would then apply. Where such remedies may not be available because of the continued covert nature of the operations, a self-contained regime is required.

13. The similarity between authorization of interception of communications and covert surveillance and the issue of a subpoena or search warrant, as suggested by some Members in our previous discussions, is in the Administration's view only limited. The considerations applicable to PII and coercive orders under the ordinances

mentioned above are also applicable. Furthermore, the information provided to the magistrate is likely to be extremely brief and usually the warrant will be executed shortly after issue.

14. Under the system proposed in the Bill, the panel judges will have to consider applications for interception of communications and the more intrusive covert surveillance against the tests set out in the Bill and on the basis of the information that the LEAs have to provide in accordance with the Bill. The standards will necessarily be judicial ones. However, the panel judges will not be sitting as a court. This means that the normal rules attendant on court proceedings will not apply. These rules include those governing legal representation, disclosure and appeal. The sensitive and covert nature of the applications necessarily makes these rules inapplicable.

15. The Bill provides for comprehensive safeguards to cater for the special nature of the applications. These include, for example, the establishment of an independent oversight authority and the protection of products obtained from interception and covert surveillance operations. As far the panel judges are concerned, their independence is safeguarded with the proviso that CE may appoint them on CJ's recommendation, and for a fixed term. Since CE may only revoke the appointment during the term on CJ's recommendation and for good cause, there should not be any question of interference with their independence. More importantly, the security of their tenure as judges is never in question.

* * * * *