(Translation) LC Paper No. CB(2)2271/13-14(01)

香港特別行政區政府
保安局

香港添馬添美道 2 號

The Government of the
Hong Kong Special Administrative Region
Security Bureau

2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.:

來函檔號 Your Ref.:

電話號碼 TEL. NO.: 2810 2632
傳真號碼 FAX. NO.: 2810 7702

8 September 2014

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

(Fax No: 2509 0775)

Dear Miss Ma,

Panel on Security
Follow-up to meeting on 3 June 2014

At the Panel on Security meeting on 3 June 2014, Members requested supplementary information on Agenda Item V "Creation of a permanent Chief Superintendent of Police post of the Cyber Security and Technology Crime Bureau". Our reply is as follows:

Requirements for the post of Chief Superintendent of Police of the Cyber Security and Technology Crime Bureau (CSP CSTCB)

Members enquired whether the post of CSP CSTCB should be assumed by an information technology specialist. Given the transnational nature of technology crime and types of offences involved (such as online shopping frauds, email scams, deception, money laundering, naked chats and publication of child pornography), we consider that the post of CSP CSTCB should be assumed by a CSP conversant with policing work, so that he may co-ordinate various tasks and set out the direction of development with an

enforcement-led approach. This arrangement would also put the Force in a better position to set objectives, devise policies and formulate long-term strategies for the maintenance of Hong Kong's overall Internet security and the combat of technology crimes.

Although the post of CSP CSTCB may not be assumed by an information technology specialist, officers with relevant computer/information technology qualifications will render support to the CSP accordingly. As a matter of fact, the Police have been recruiting officers with relevant computer/information technology qualifications to join the CSTCB. At present, 94% of the officers under the Technology Crime Division (TCD) have such qualifications, while the rest of the officers have received internal professional training and possess relevant experience.

Besides, in collaboration with the Police College, the TCD's Training Team organises regular internal professional training programmes which cover topics like technology crime investigation skills and computer forensic examination. Such programmes are offered to maintain TCD officers' professional capability in investigation, intelligence gathering and analysis, computer forensic examination and training. Overseas visits are conducted from time to time for officers' participation in training on technology crime investigation skills, computer forensic examination, etc. Apart from gaining international experience, officers may share their experience and insights with other law enforcement agencies' experts in order to acquire the most advanced knowledge.

Creation of an additional of some 70 non-directorate posts

For establishing the new CSTCB, the TCD of the Commercial Crime Bureau (CCB) will be hived off with the permanent redeployment of 106 posts from the CCB to CSTCB. Moreover, an additional 74 non-directorate posts, comprising 71 disciplined posts and 3 civilian posts, will be created.

The two divisions under the CSTCB, i.e. the TCD and the Cyber Security Division (CSD), will be headed by a CSP and a Senior Superintendent.

As there will be a considerable expansion in the CSD of the CSTCB, most of the new posts (51 disciplined officers ranked from Police Constable to Superintendent of Police) will be created in the three sections under the CSD. These sections, with the increase of manpower, will enhance cyber watch and protection, render immediate and emergency

responses/actions against cyber attacks, as well as strengthen communication and collaboration with relevant overseas and local stakeholders for bringing improvements to the investigation work. The CSD, with the additional manpower, may then significantly shorten the network security auditing cycle of critical infrastructures as a way to prevent and tackle cyber attacks in a more comprehensive and effective manner. The increase of staff will also enable the Police to conduct analysis and thematic researches on cyber attacks.

On another front, 19 disciplinary posts (ranked from Police Constable to Chief Inspector of Police) and 3 civilian posts will be created under the TCD. A new investigation team will also be set up under the TCD for enhancing investigations into massive cyber attacks and major cyber security incidents as well as combatting syndicated and high-tech crimes. In addition, an advance training team will be established to provide more intensive training in cyber attack incidents and investigation skills.

Privacy of the Public

Some Members expressed concern on whether the CSTCB would conduct any surveillance on the public and whether freedom of speech would be restricted by its work. In relation to technology crime investigations, the Police will not request to have access to the computer systems of internet service providers. Furthermore, for the purpose of investigating technology crimes, the Police will not access the computer systems of any organisations or individuals without legal authorisation or consent of the persons concerned.

Yours sincerely,

(Mrs Millie Ng)
for Secretary for Security

c.c.: Commissioner of Police
(Attn: Assistant Commissioner of Police (Crime)) Fax No: 2528 2284