(Translation)

LC Paper No. CB(2)826/13-14(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

6 February 2014

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

(Fax No: 2185 7845)

Dear Miss Ma,

In connection with Members' request for written information on the new Cyber Security and Technology Crime Bureau (CSTCB) at the meeting of the Panel on Security on 20 January 2014, I am authorised to reply as follows:

The Technology Crime Division (TCD), under the Commercial Crime Bureau (CCB) of the Hong Kong Police Force (HKPF), is mainly tasked with detecting and preventing technology crimes, supporting other police formations in technology crime investigations, handling computer exhibits and providing contingency support and protection to information systems of critical infrastructure in case of cyber security incidents.

According to the HKPF, the number of technology crime reports significantly increased from 1 506 in 2009 to 5 133 in 2013, among which the figures of "online business fraud" and "unauthorised access to computers" increased by 260% and 350%, thus giving rise to public concern.

In the 2014 Policy Agenda, the Chief Executive proposed the upgrading of the TCD of the HKPF CCB to a CSTCB in order to strengthen the protection of information systems of critical infrastructure and enhance the Police's capability in preventing and combating technology crimes. The new CSTCB will increase the Police's overall capability in handling cyber security and combating technology crimes through its diversified services and expanded role in cyber security. Its functions include:

- detecting advanced and complicated technology crimes;
- conducting training on cyber security and technology crimes;
- collaborating with local and overseas stakeholders;
- undertaking thematic researches and cyber security audits;
- analyzing intelligence in relation to cyber attacks;
- detecting cyber security incidents and exercising emergency response capability; and
- examining the handling procedures, developments and mode of operation of current technology crimes and studying countermeasures against cyber attacks.

When conducting investigations into technology crimes, the Police may, having regard to the nature of a case, request local and overseas internet service providers (ISPs) to provide users' information, login records and so forth in accordance with section 58(1)(a) of the Personal Data (Privacy) Ordinance (Cap 486), i.e. for the purpose of crime prevention and detection, for locating witnesses, evidence or suspects. In relation to technology crime investigations, the Police will not request to have access to ISPs' computer systems. In addition, the Police will not access the computer systems of any organisations or individuals without legal authorisation or the 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