(Translation)

LC Paper No. ESC104/14-15(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.: SBCR 1/1805/13 Pt.4

來函檔號 Your Ref.:

電話號碼 TEL. NO.: 2810 2632
傳真號碼 FAX. NO.: 2877 0636

13 July 2015

Clerk to the Establishment Committee
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong
(Attn: Mr Jason Kong)

Dear Mr Kong,

Your letter to the Financial Services and the Treasury Bureau dated 30 April 2015 was referred to us for further actions. In relation to the matters raised therein in follow-up with the meeting of the Establishment Subcommittee on 29 April 2015, our response is at Annex.

(Mrs Millie Ng)
for Secretary for Security

w/encl. (3 pages)

c.c.
CP (Attn: Ms Irene Ho, CSP (Crime HQ)(Crime Wing)
Mr Francis Chan, SSP CSTCB)

Annex

Follow-up matters to the meeting of the Establishment Subcommittee on 29 April 2015

Security of the Cyber Security Centre

The Cyber Security Centre ("CSC") plays an important role in defending against and responding to major cyber attacks in Hong Kong. When drawing up security measures for the CSC, the Police have to take into consideration a basket of factors, including data confidentiality requirement, security technologies involved, effective software and hardware required, safety of the operation site and so forth. To ensure their capability in managing cyber security of Hong Kong, the Police must critically and thoroughly formulate CSC's physical and virtual security initiatives. Among such initiatives, the operating procedure, operation, technology and capability of the CSC should be kept strictly confidential to prevent the CSC from becoming a target of hackers' attack or intrusion, as well as to ensure its capability in defending against major cyber attacks.

2. Moreover, the CSC is required to process and analyse sensitive data in its day-to-day operation, including the flow (not the content) of data traffic as well as the data in relation to cyber attacks that stakeholders of critical infrastructures (e.g. computer systems of banking and finance services, traffic and maritime services, communication services, public services and government services) are willing to provide. The collaboration between the CSC and such stakeholders is based on a mutual confidentiality agreement.

3. On account of the aforesaid reasons, matters in relation to the CSC are handled by the Police in strict compliance with the "need-to-know" principle since the full commissioning of the CSC. This security principle is of paramount importance in guarding against the leakage of CSC's classified data, including those about CSC's capability, method, system operation and technology in support of law enforcement.

4. Owing to CSC's confidentiality and sensitivity, the Police generally do not entertain the request for visiting the CSC; approval of any person's access to the CSC is determined by the Police on the "need-to-know" principle. Since the full commissioning of the CSC, only its staff, officers with operational needs and relevant policy makers are allowed access to it.

Briefing on the Work of the CSC

5. The SAR Government respects Legislative Council Members' duty in monitoring the Government and is pleased to expound on the work of the CSC. At the meeting of the Establishment Subcommittee on 29 April 2015, the Government expressed time and again that it would be willing to arrange police officers to give Members a special briefing for their further understanding of CSC's work. We have to reiterate that, so long as Members agree to such an arrangement, the Police are pleased to organise a briefing for Members before submission of the proposal to the Finance Committee for consideration.

Figures of prosecution and conviction in respect of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance

6. Section 161(1) of the Crimes Ordinance reads as follows:

Any person who obtains access to a computer-

(a) with intent to commit an offence;
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another,

whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

7. Figures of prosecution and conviction in respect of "access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance between 2011 and 2014 are set out below.

Year	Number of prosecutions	Number of convictions
2012	39	32
2013	55	50
2014	86	80

8. The above are the overall prosecution and conviction figures of the offences under section 161. The Government does not have separate figures[Note] of the respective offences under the four subsections, i.e. (a), (b), (c) and (d).

Security Bureau
Hong Kong Police Force
July 2015

Note In order to analyse Hong Kong's overall law and order situation and crime trend, and to understand the profile of our criminal justice system, law enforcement agencies (LEAs) and the Judiciary maintain various crime-related statistics, such as numbers of cases and arrestees, as well as figures of prosecutions, convictions, penalties imposed, etc. in respect of different offences. The figures recorded are the overall figures of various offences, and therefore separate figures are not maintained for the offences under the respective subsections. For example, there are two subsections under the offence of "burglary" (Section 11 of the Theft Ordinance), namely:

11(1)(a) a person enters any building or part of a building as a trespasser and with intent to commit any such offence as is specified in the relevant subsection, including stealing, inflicting on any person therein any grievous bodily harm or raping any woman therein, or doing unlawful damage to the building or anything therein; and

11(1)(b) having entered any building or part of a building as a trespasser he steals or attempts to steal anything in the building or that part of it or inflicts or attempts to inflict on any person therein any grievous bodily harm.

A person involving in the crime under subsection (a) or (b) commits the offence of "burglary". With respect to the statistics compiled and the figures maintained for "burglary", LEAs only maintain an overall figure of such an offence (i.e. no separate figure for either subsection (a) or (b)), without a breakdown of the respective figures for subsections (a) and (b). As far as section 161 is concerned, there are four subsections, i.e. (a), (b), (c) and (d). Regarding the statistics of the offences under section 161, as in the case of "burglary", LEAs and the Judiciary only maintain an overall figure, instead of a breakdown of the respective figures for the four subsections.