立法會
Legislative Council

LC Paper No. CB(2)949/15-16(06)

Ref : CB2/PL/SE

Panel on Security

Information note prepared by the Legislative Council Secretariat for the meeting on 1 March 2016

Information technology infrastructure and Command and Control Communications System of the Hong Kong Police Force

Information technology infrastructure

According to the Administration, the Hong Kong Police Force adopts a distributed information technology ("IT") infrastructure to support all computer facilities connected to the Local Area Networks ("LANs") in the police premises covering Police Headquarters, regions, districts, divisions and offices. These LANs are riding on the Police Data Network ("PDN"), which is the Force-wide data communication network for the IT applications. Over the years, the IT infrastructure has been incrementally enhanced to cater for the new developments of the major systems.

2. In view of the increasing IT needs of police duties in terms of data accessibility, mobility and security, the Administration proposed in April 2010 to enhance the Police's IT infrastructure by employment of virtualisation technology, which referred to a server computing model under which virtual workstations running on a remote central server would replace personal computers, and all of the programmes, applications processes and data used were kept and run centrally on the server ends. With the adoption of virtualisation technology, police officers could access case information securely in their offices as well as other locations. There was no need for them to bring home the external thumb drives containing case-related information or data for work purposes, and this would considerably reduce the risk of data leakage. The Finance Committee ("FC") approved at its meeting on 14 May 2010 a new commitment of $40,716,000 for the Police to enhance its IT infrastructure by introducing the virtualisation technology.

3. When the above funding proposal was considered at the FC meeting, members expressed grave concern about whether the Police had put in place adequate controls and security for data protection. Members were advised that the virtual workstation was proposed specifically to address the problems of data protection and IT security within the Force. Under the new virtualisation infrastructure, all data was processed and stored in the central server, and only screen image could be transferred to front-line terminals (which had no processing and storage power) through the secured data channel. There were two levels of data protection/security device under the virtual workstation infrastructure, i.e. the information processed under the virtual workstation could be channelled back to the central servers, and there were different levels of information access control permitting only the authorised personnel to access the central servers to read the information and/or to work on the information therein. Users at public places or their own residence could not access the internal networks of the Police or the data stored in the central servers without the installation of Virtual Private Network and related software, which could only be provided upon authorisation.

4. Members were further advised that data related to crime intelligence was not stored in the central server of the virtual workstation. Information accessible by the virtual workstation was confined to those related to the daily work of police officers. Nonetheless, the Police had adopted high data security protocols and authenticated techniques to ensure protection of sensitive information transmitted on the Internet. Clear guidelines had also been issued to police officers to remind them to be vigilant in handling confidential information and classified documents.

Command and Control Communications System

5. The Third Generation Command and Control Communications System ("CCIII") currently used by the Police has come into operation by phases since December 2004. According to the Administration, CCIII consists of four major components -

(a) an Integrated Communications System with voice and data capabilities based on the terrestrial trunked radio standard;

(b) a 999 Emergency Telephone System with automatic emergency caller number and location identification capability;

(c) a Mobile Computing System allowing officers to access necessary information from their radio handsets and/or mobile data terminals; and

(d) an Automatic Vehicle Location System that allows dispatchers to better allocate resources to attend emergency incidents as well as a Geographic Information System that allows the emergency call takers and dispatchers to more quickly and accurately identify the location of emergency incidents and police vehicles notably Emergency Unit vehicles, Traffic vehicles (including motorcycles), Marine Police cars and Police Training Unit command vehicles.

6. CCIII supports an integrated command and control environment that includes radio, telephone, incident handling, voice logging, automated action cards, and support for external interfaces to computer systems in selected government departments. Its security features, which include encryption and authentication of users, can prevent eavesdropping by unauthorised elements.

7. When FC discussed the Administration's funding proposal for the acquisition of CCIII at its meeting on 22 June 2001, members were advised that the expected lifespan of CCIII was over 10 years. The system was a digital radio infrastructure built to an open standard which allowed an incremental approach to future system enhancement. Equipment such as beat radios was not proprietary to a particular vendor and could be procured from open markets at lower costs.

8. The Administration will brief the Panel on Security on its proposal to upgrade the Police's IT infrastructure and applications and to replace CCIII of the Operations Department at the meeting on 1 March 2016.

Council Business Division 2
Legislative Council Secretariat
25 February 2016