LC Paper No. CB(2)1544/06-07(01)

For information

Legislative Council Panel on Security

Replacement of the Radio System of the Operations Wing of the Hong Kong Police Force (HKPF) Supplementary Information

Background

At the meeting of the Panel on Security on 6 March 2007, the Administration undertook to provide further information on how to ensure the security of the proposed radio system for the Special Duties Unit (SDU) of the Police when the maintenance is outsourced.

Security requirements

2. The proposed radio system for the SDU will adopt an established international standard[1]. This standard is widely adopted by other public safety agencies around the world for their communications systems. The security requirements of this standard necessitate the use of cryptographic-based security systems for the protection of sensitive and valuable data, and place importance on in-built security features of the equipment. There is no requirement for the maintenance of the hardware to be kept in-house.

3. Information transmitted through the radio handsets is subject to "end-to-end" digital encryption. During the transmission, the information (i.e. voice) is encrypted and at the receiving end it is decrypted. The information is not "stored" in the handset as such. Rather, once it is transmitted it is "spent". The proposed radio equipment will be so built to allow the necessary encryption and decryption ***with the necessary encryption keys***. The keys are not physical keys, but are codes generated and stored by the Police into a "key loader" device for onward loading into the handset. The handsets are built with such safety features that if someone attempts to take a handset apart to access the information, the tampering will result in the automatic erasure of the encryption keys in the handset. The Police will have physical custody of the encryption key information, which will be stored in the safe of a specified officer and accessible only by

[1] The standard is the Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) issued on 25th May 2001 by the US National Institute of Standards and Technology (NIST).

him/her. Moreover, operating the key loader requires a password, and only the Police will have access to it. A key management process will also be put in place whereby the encryption keys are changed from time to time through reprogramming the handsets with the key loader on a schedule determined by the unit commander.

Keeping of inventory

4. Apart from those (few) radio handsets that may need to be sent to the contractors for maintenance or repair, all handsets are kept by the Police at all times. There are also very stringent guidelines on the safekeeping of the handsets. The Police will carry out frequent checks to account for the whereabouts of the handsets. Hence handsets found missing for whatever reason will be readily identified. If a handset is lost, procedures for changing the encryption keys of all remaining handsets will be activated immediately to minimize any possible risk of unauthorized access to information transmitted by the system.

Repair arrangements

5. The Police will erase all encryption keys in the handsets and reprogram them with dummy information (including frequencies) before they are given to the contractor for repair service. When the repaired handsets are returned from the contractor, the Police will perform tests on them for integrity assurance before reprogramming them with valid encryption keys and other information such as frequencies. If there has been any tampering during the repair process, it will be detected from the tests.

6. Unlike computers, with radio handsets there is no space, either physically within the compact size handset or memory-wise in the ‘chip’, that could allow an extra electronic component or software ‘bug’ to be implanted in the handset. The threat of compromise to the integrity of radio communication by the contractor tampering with the handsets passed to them for repair therefore would be very low. The servicing of most other components of the new system is done on site, under the supervision of the Police.

Greater efficiency through outsourcing

7. Currently, the Police do not have the level of professional expertise required to efficiently service the various components of the proposed system. To acquire the necessary training would require the cooperation of the contractor. In

addition, unless the Police were to assume the manufacturing role as well, they would still have to look to the contractor or some other suppliers for the spare parts. It would not be practicable for the Police to assume the servicing role without affecting the effectiveness of the system. It is indeed in line with the international trend for such servicing and maintenance to be outsourced. With the robust security requirements and procedures in place, we consider that the risk of outsourcing is very low and acceptable.

Security Bureau
Hong Kong Police Force
April 2007