Telecommunications Regulatory Affairs Advisory Committee

Proposed Update of the "Security Guidelines for Next Generation Networks"

PURPOSE

This paper seeks Members' views on the proposal to update the "Security guidelines for next generation networks" ("NGN Guidelines") in light of technology developments.

BACKGROUND

Guidelines for network security

2. Telecommunications licensees are required under General Condition 5.1 of the Unified Carrier Licence ("UCL") and the Services-based Operator Licence ("SBO Licence") to provide a good, efficient and continuous service in a manner to the satisfaction of the Communications Authority ("CA"). Pursuant to Special Conditions ("SC"s) 1.2(a) and (c) of the UCL, and SCs 13.1(a) and (c) of the SBO Licence, the CA may issue guidelines for the purpose of providing practical guidance to the licensees in respect of the provision of a satisfactory service and to ensure the protection and promotion of the interests of consumers of telecommunications goods and services. Section 32D of the Telecommunications Ordinance also empowers the CA to prescribe standards and specifications to facilitate correct, efficient and reliable operation of telecommunications.

3. The Office of the Communications Authority ("OFCA") has been developing guidelines setting out the best practices on network security for operators to follow. To this end, the "Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi

Service"[1] were issued in 2007 while the NGN Guidelines[2], which apply to packet-based fixed networks and the fourth generation mobile ("4G") networks, were issued in 2010 (with only minor textual amendments made thereafter).

THE NEED FOR UPDATE

4. Almost nine years have passed since the NGN Guidelines were first formulated. With the advent of the fifth generation mobile ("5G") era and the new emerging technologies, it is expected that 5G networks will underpin a wide range of new communications services and smart city applications, including enhanced Mobile Broadband ("eMBB"), massive Machine-Type Communications ("mMTC"), and Ultra-Reliable and Low Latency Communications ("URLLC"). It will also provide a more sophisticated communications platform for supporting massive deployment of Internet of Things ("IoT") devices and smart applications.

5. New technologies are also expected to be adopted for the provision of new 5G services and applications, which include -

(a) **Network Slicing**: This enables mobile network operators ("MNOs") to create and provide multiple logical networks over their physical infrastructure, which will facilitate development of new services for greater flexibility, higher efficiency and lower costs;

(b) **Network Functions Virtualisation ("NFV")**: NFV enables MNOs to manage and expand their network capabilities using software based applications installed in distributed physical infrastructure. It will make it easier to carry out network functions such as load-balancing, network scaling, and migration of network resource across distributed hardware resources. MNOs can in future upgrade the latest software without service

[1] "Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service" (https://www.coms-auth.hk/filemanager/statement/en/upload/388/gn182016e.pdf).

[2] "Security Guidelines for Next Generation Networks" (https://www.coms-auth.hk/filemanager/statement/en/upload/401/gn012017e.pdf).

interruption to their customers;

(c) **Software-defined Networking ("SDN")**: SDN enables MNOs to configure and to manage networks and services through software rather than specific hardware. SDN optimises network resources and enables networks to respond quickly to changes in traffic or individual applications; and

(d) **Edge Computing**: It is a distributed computing system in which a significant part of the computation will be performed on distributed devices (e.g. devices equipped with communications module and computation function installed in vehicles) at the edge of the network rather than in a centralised cloud environment. This will support applications that may require ultra-low latency (of about 1 millisecond) such as autonomous driving.

THE PROPOSAL

6. Along with the opportunities of new services and applications, the above new technologies may also bring about new security threats in addition to those common to the 4G networks (e.g. unauthorised use of service, unauthorised tampering with data, insecure access to information and data, interruption of services, destruction of information and/or network resources, etc.). We therefore consider it necessary to review and, where appropriate, update the NGN Guidelines to ensure that our future 5G networks or newer generations of Internet Protocol ("IP") networks will continue to be protected against potential security threats. This in turn will ensure the provision of continuous, secure and reliable services to the consumers.

7. In line with our usual approach, we will take into account latest international and regional standards, specifications and best practices in reviewing the NGN Guidelines. In this connection, we understand that studies have been carried out by standard organisations and industrial bodies around the world (e.g. 3rd Generation Partnership Project ("3GPP"), 5G Infrastructure Public Private Partnership ("5G PPP"), European Telecommunications Standards Institute ("ETSI"), etc.) on ways to better

protect the telecommunications network in the 5G era. Subject to any views and initial comments from Members, we will draw reference from the suggestions of these organisations in updating the NGN Guidelines. The draft additions/amendments to the NGN Guidelines will be circulated to relevant operators for comments before we finalise them for approval of the CA.

Office of the Communications Authority
March 2019