LCQ8: Information security of using certain Chinese telecommunications products

Following is a question by the Hon Alvin Yeung and a written reply by the Secretary for Innovation and Technology, Mr Nicholas W Yang, in the Legislative Council today (January 16):

Question:

It has been reported that in recent months, the governments of a number of countries (including the United States, Japan and Australia) have banned, on national security grounds, their respective government agencies and telecommunications service operators from using the telecommunications equipment supplied by Huawei Technologies Co. Ltd (Huawei) and ZTE Corporation (ZTE). Regarding the information security in relation to the use of these two companies' equipment by the Government, will the Government inform this Council:

(1) of the details of the products of (i) Huawei and (ii) ZTE being used by various government departments (set out separately in tables of the same format as the table below); and

	Type of products	Quantity	Total value	Purpose	Year of purchase	Government department
1.						
……						

(2) whether it inspected, in the past 12 months, those Huawei and ZTE products being used by various government departments to see if there were hidden backdoors or functions which enabled unauthorised persons to steal the information in Government possession; if it did, of the outcome, and the follow-up actions taken by the Government?

Reply:

President,

At present, in procuring network equipment products, government departments can either conduct their own tendering exercises or select suitable products from the Standing Offer Agreement for the Supply of Network Products and Server Systems (SOA) under the Office of Government Chief Information Officer (OGCIO). In formulating the SOA, the OGCIO takes into account mainly product functionality, compatibility, relevant technical and security standards, and support offered by the suppliers. There are no

restrictions on the brand of equipment.

Replies to each part of the question are provided as follows:

(1) For the period from February 2016 (commencement date of the prevailing SOA) to November 2018, government departments procured around 190 Huawei Technologies Co. Ltd products through the SOA including network switches (for connecting equipment on a network), routers (for connecting different networks) and accessories (fibre transceivers and cables for connecting fibre optics, and fan modules for cooling equipment). The total expenditure is around $1.76 million.

The contractors in the prevailing SOA do not offer any ZTE Corporation products.

For network equipment procured by individual departments through their own tendering exercises, relevant information such as product categories and expenditure is kept by the departments and the OGCIO does not have statistics in this regard.

(2) In drawing up the arrangements and procedures for procuring information and communication products, the Government makes reference to international and industry standards including information security, and stipulates the requirements for safeguarding information systems and data assets to ensure the security of government information systems and data as well as to protect the privacy of the general public. At present, the network equipment brands and models procured by the Government are widely used by other international cities and should not have a backdoor programme or other inappropriate functions. Therefore, the prevailing procurement procedures do not include additional checking in this respect.

Regarding government-wide risk management of information technology security, the OGCIO has worked together with relevant departments to formulate a comprehensive set of policies and guidelines, management framework and technical measures, and closely monitor the operation of government information systems and networks so as to detect and intercept various potential security threats and assess the risks of cyber attacks. Such guidelines, management framework and technical measures are applicable to all products or brands.

To ensure the security of government's information systems and data as well as to protect privacy of the general public, government departments must perform independent information security risk assessments and audits for their information systems and network facilities before commissioning and during operation on a regular basis. They will make improvement as necessary to ensure the relevant information systems and network facilities comply with the security requirements and regulations. Furthermore, in order to ensure the security of data asset, confidential and restricted data must be encrypted in storage or transmission.

The OGCIO will also monitor closely the information disseminated by the

information security industry and computer emergency response teams from all over the world, including security threats and trends of cyber attacks. Having regard to the actual circumstances, the OGCIO will assess and plug the potential security risks, including risks of product vulnerabilities or data leakage.