香港特別行政區政府

政府資訊科技總監辦公室

OFFICE OF THE
GOVERNMENT CHIEF INFORMATION OFFICER

THE GOVERNMENT OF THE HONG KONG
SPECIAL ADMINISTRATIVE REGION

本函檔號 Our Ref. : GCIO-055-074-002-001
來函檔號 Your Ref. :
電話 : 2867 4608
傳真 : 3153 2665
電子郵件 : vkmchou@ogcio.gov.hk

29 August 2017

Clerk to the Finance Committee
(Attn: Ms Anita SIT),
Legislative Council Complex,
1 Legislative Council Road,
Central, Hong Kong

Dear Ms SIT,

Centrally Managed Messaging Platform

I refer to the e-mail dated 13 July 2017 from the Legislative Council ("LegCo") Secretariat to the Financial Services and the Treasury Bureau requesting for information from the Government. We noted that the enquiry was raised by Mr Nathan LAW Kwun-chung who has been declared by the Court to have been disqualified from assuming and entering on the office of a LegCo member and have vacated such an office since 12 October 2016. Nevertheless, since the letter was issued by the LegCo Secretariat, we treat the matter as the business of LegCo and thus provide a reply, but entirely without prejudice to the Government's position that Mr Nathan LAW Kwun-chung is not entitled to act or claim to act as a member of LegCo under the law. After consulting the relevant policy bureaux, our reply is given below. The Government reserves its rights concerning all matters relating to any relevant appeal proceedings.

(1) The feasibility study conducted by the consultant engaged by the Office of the Government Chief Information Officer ("OGCIO") reveals that government agencies of a number of advanced countries or cities (e.g. the United States) set up their centrally managed messaging systems essentially on top of existing communications software available in the market.

(2) According to the definition in Government IT Security documents, "availability" means that an information system is accessible and usable on demand by authorised persons. 99.95% availability means that the time that the system cannot provide services is less than 22 minutes a month. Having considered cost-effectiveness and user requirements, the Government considers that 99.95% availability is an appropriate and a very high level of system services. Its performance pledge is higher than the 99.5% pledged by public cloud e-mail service providers. Generally speaking, only individual system components such as servers, communications network equipment can achieve 99.999% or even higher availability. As far as the whole system is concerned, the performance pledge of 99.95% availability is already a very high level since collaboration among different components is required.

(3) According to the system design requirements stated in the tender documents, the appointed contractor ("the Contractor") has to provide Full Resilience with Disaster Recovery ("DR") Facility, including backup servers, for the Centrally Managed Messaging Platform ("CMMP") at the government data centre in another location. When necessary, the Contractor has to resume service within 10 minutes.

(4) The recommendations of the feasibility study, including the relevant resilience and DR requirements of the system, have been included in the open tender documents of CMMP. The contents of the tender documents are available at the following URL:

https://www.ogcio.gov.hk/en/business/tender_eoi_rfp/doc/GCIO-055-074-002-001-Tender(v1.2).zip

(5) The Government's current e-mail system architecture was built on a decentralised model which is difficult to leverage on technology advancement (such as cloud computing) in a timely manner, and adopting the latest security protection functions (e.g. security patches and encryption standards) in a concurrent manner. This would limit the ability of government bureaux and departments ("B/Ds") to tackle the increasing cyber security risks. In addition, computing resources may not be properly integrated and optimally utilised in maintaining and managing such decentralised system by individual B/Ds. CMMP, which will be centrally managed, will replace the existing decentralised e-mail systems and obviate the need for B/Ds to support and upgrade the individual e-mail systems on their own. B/Ds can also achieve a consistent level of information security protection which meets or even exceeds industry standards and will

be more robust against cyber attacks. As far as the comparison between cloud servers and internal servers is concerned, the use of cloud servers will not only enable dynamic expansion to meet user demands, but also reduce the number of servers required from about 320 at present to some 80, saving space and reducing electricity consumption by two-thirds. The centralised model of CMMP could further support integration of other collaboration tools such as instant messaging and file sharing, enabling B/Ds to make use of the latest technologies in a timely and effective manner.

(6) & (7) At present, different B/Ds mainly deploy their internal staff to undertake the daily operation and maintenance of their messaging systems, and engage contractors on their own to jointly manage the systems having regard to individual circumstances. The Contractor of CMMP has to provide services for the daily operation and maintenance of CMMP together with OGCIO for 7 years.

All communications over the network relating to CMMP will be encrypted to safeguard information security. When handling e-mails containing confidential information, users will encrypt each confidential e-mail separately with their own digital certificates to ensure that only the sender and the recipients can read the e-mails. Moreover, the accounts of CMMP will be protected by the management system and an independent audit trail mechanism that can record activities in the system. No unauthorised persons, including Contractor staff, can access user data. As for the daily operation and maintenance, all work involving sensitive information (including user data) will be handled by the staff of OGCIO as in the existing arrangements. Contractor staff cannot access such information.

(8) Security specifications of CMMP conform to the Government's Security Regulations as well as IT security policies and guidelines. The primary server and DR facilities of CMMP will be housed at the government data centres in different districts.

(9) As the Central Government Offices ("CGO") is supported by a robust network infrastructure, and staff of these 22 B/Ds are often required to handle sensitive information, early implementation of CMMP will enable these B/Ds to achieve a consistent level of security protection which meets or even exceeds industry standards. Hence, it is recommended in the feasibility study that CMMP be first implemented in the B/Ds and their offices which are based in CGO.

Upon implementation of CMMP, we will review its effectiveness and sum up the

experience. If CMMP is confirmed to be effective, we will submit a funding proposal to the Finance Committee ("FC") for extending CMMP to other B/Ds.

(10) Having regard to the circumstances of individual projects, B/Ds have all along, after conducting a risk assessment, considered adopting "parallel tendering" as appropriate for expediting the commencement of works. This arrangement has all along been effective. OGCIO considers that parallel tendering would expedite the commencement of the CMMP project after conducting a risk assessment. After obtaining approval from the Secretary for Innovation and Technology, OGCIO launched the open tendering exercise of CMMP at the end of March this year. OGCIO has also stated in the tender documents of CMMP that funding approval for the project has yet to be obtained, and tenderers have been reminded that the Government will not be responsible for the cost for their preparation of tenders. According to the procedures, OGCIO will only award the contract after obtaining FC's funding approval. Therefore, no additional tendering costs have been involved in this parallel tendering arrangement.

(11) B/Ds are required to identify, create, collect adequate but not excessive records (including e-mail records) to meet operational, policy, legal and financial purposes, and to maintain accurate and complete documentation of the Government's policies, procedures, decisions and business transactions as reliable evidence according to the guidelines issued by the Government. Apart from B/Ds which have successfully implemented the electronic recordkeeping system, all B/Ds should print out e-mail records and file them in the appropriate paper file system. Besides, B/Ds are required to retain and handle records according to the established records retention and disposal schedules. The above requirements will not be changed arising from the rollout of CMMP.

(12) The public can put up requests for government information including e-mail records to government departments under the Code on Access to Information ("the Code"). The Code defines the scope of information that will be provided, sets out how the information will be made available either routinely or in response to request, and lays down procedures governing its prompt release. According to the Code, when handling a request for information, government departments should provide the information requested unless there are sufficient reasons for refusing the disclosure of such information under Part 2 of the Code. Details are available at the following URL:

http://www.access.gov.hk

(13) Since LegCo is an independent body and its e-mail system has all along been independent from government departments, LegCo's e-mail system is not included in this project.

Yours sincerely,

(Vinci CHOU)
for Government Chief Information Officer

c.c.
Secretary for Innovation and Technology (Attn: Mr Ricky CHONG)
Secretary for Financial Services and the Treasury (Attn: Ms Bella MUI, Mr Herman SO)