

**For discussion
on 13 March 2017**

**Legislative Council Panel on
Information Technology and Broadcasting**

Implementation of Centrally Managed Messaging Platform

Purpose

This paper seeks Members' support for the implementation of a new Centrally Managed Messaging Platform ("CMMP") in the Government to replace the decentralised email system currently in operation in bureaux/departments ("B/Ds").

Background

2. The Government's current email system architecture was built about 20 years ago based on a decentralised model, under which each B/D sets up and manages its own email system. While the Government has put in place an information security framework with sufficient checks and balances, a system set up with a decentralised model is less capable of leveraging on the technology advancement in a timely manner. For example, under the existing server-centric email system design, when performing system upgrade, B/Ds may not be able to adopt the latest technology and leverage on scalable infrastructure, including cloud computing which has emerged in recent years. Making use of the high computing power possessed by the infrastructure based on cloud computing technology, services are delivered through high speed networks. To achieve economies of scale, cloud computing needs to be based on a centrally managed system for optimising resources and enhancing scalability.

3. Furthermore, under a decentralised model, due to the differences in resources availability and work priorities, B/Ds may not be able to adopt the latest security protection functions (e.g. security patches

and encryption standards) in a concurrent manner, affecting their ability to tackle the increasing cyber security risks. Moreover, individual B/Ds may not have sufficient manpower resources and relevant expertise to deal with the ever changing cyber security risks.

4. With regard to maintenance and on-going system support, B/Ds need to allocate manpower resources to take up the management and support work. As some email servers may be scattered across different office locations of B/Ds, management would be more difficult. Also, the computing resources may not be properly integrated and optimally utilised.

5. Nowadays, instant messaging services are very popular. Making use of this function, users can instantly communicate thereby enhancing work efficiency. However, the existing email system of B/Ds cannot provide or integrate instant messaging services, and as a result staff cannot perform official duties outside offices using instant messaging. Instant messaging services provided by third party service providers may not be suitable for communication on official matters, especially for those involving sensitive information. On the other hand, under the existing system, it is common practice for users to attach documents in their emails and store in the mailboxes in the email system, making it difficult and time consuming in searching and retrieving the documents.

Proposal

6. In view of the above situation, the Office of the Government Chief Information Officer (“OGCIO”) commissioned a consultant in 2016 to study a government messaging platform which could meet the needs of today and the future. The study recommended building a new Government messaging system based on a centralised model which is expandable to support integration of other collaboration tools such as instant messaging and file sharing. The messaging platform will enable B/Ds to make use of the latest technologies and tackle the increasing cyber security risks timely and effectively.

7. We agree with the study's recommendation and plan to implement CMMP initially for the B/Ds located in the Central Government Offices and their related sub-offices (as listed at Annex). A comparison of the characteristics of the existing email system and CMMP is as follows -

	Existing Email System	CMMP
1. Email Communication	Encryption for restricted classification of emails can meet the basic security requirements	Strong encryption for emails of restricted classification, compliant with the latest international standards
2. Compatibility with other communication and collaboration tools	Incompatible with other communication and collaboration tools (e.g. unified communication and file sharing)	Compatible with other communication and collaboration tools (e.g. voice mailbox, unified communication and file sharing)
3. Instant Messaging	Not support mobile instant messaging	Support mobile instant messaging up to confidential classification
4. Reliability and Availability	Servers distributed in different office locations of B/Ds, more difficult to ensure availability and more vulnerable to security attacks	Cloud servers with 99.95% availability, more robust against security attacks; full resilience with disaster recovery facility
5. Environmental Friendly and Energy Saving	Distributed servers resulting in duplicate resources, without versatile system management	Centralised cloud servers scalable to meet user demand, more environmental friendly and energy saving, and with versatile system management

	Existing Email System	CMMP
6. Information Security	Managed by individual B/Ds, difficult to achieve a consistent level of security protection	Can achieve a consistent level of security protection among different B/Ds meeting or even exceeding industry standards
7. Economies of Scale	Duplicated support resources, cannot achieve economies of scale	Economies of scale with central support; high availability, ease of use and secure

Anticipated Benefits

8. CMMP, which will be centrally managed, will replace the existing decentralised email system of B/Ds and avoid the need for them to independently support and upgrade the individual email systems. On information security, B/Ds can achieve a consistent level of security protection meeting or even exceeding industry standards and will be more robust against cyber attacks. Moreover, CMMP will provide support 24 hours a day, 7 days a week, with 99.95% availability (i.e. the system will be in normal operation for 99.95% of the time), and possess disaster recovery capability.

9. CMMP will adopt scalable cloud servers which can be dynamically expanded to meet user demands. The total number of servers will be reduced, saving space and reducing electricity consumption. Also, we will use servers of the latest model with higher energy efficiency to reduce carbon footprint.

10. By adopting the latest industry standards, CMMP will be compatible with a series of collaboration tools (e.g. unified communication with text, voice, image and video contents, and file sharing) and will fully support mobile instant messaging to meet today's business needs and enhance work efficiency.

11. CMMP will also open up the opportunity for B/Ds to establish digital workplace, and through integrating with collaboration tools such as instant messaging, video conferencing, document storage and file sharing, introduce new work mode to streamline office workflow and strengthen information security. The above functions will enhance the operational efficiency and productivity of B/Ds, as well as achieving economies of scale for the Government.

12. Taking into consideration the scale of the proposed project, CMMP will initially be implemented in B/Ds located in the Central Government Offices and their related sub-office users. CMMP will be gradually expanded in future to cover Government departments in other locations for better economies of scale.

Financial Implications

Non-recurrent Expenditure

13. The proposal will incur a total one-off cost of \$252.21 million in four financial years from 2017-18 to 2020-21, with breakdown as follows:

	(\$ million)				
Item	2017-18	2018-19	2019-20	2020-21	Total
(a) Hardware	7.19	-	19.78	8.99	35.96
(b) Software	8.29	-	22.79	10.35	41.43
(c) Implementation Services	18.91	-	52.90	24.38	96.19
(d) Contract Staff	7.64	15.27	15.27	7.63	45.81
(e) Others	1.52	0.60	5.32	2.46	9.90
(f) Contingency	-	-	-	22.92	22.92
Total	43.55	15.87	116.06	76.73	252.21

14. The estimated \$35.96 million under item (a) above is for procurement of computer hardware, including servers, network facilities, security modules and backup equipment.

15. The estimated \$41.43 million under item (b) above is for procurement of computer software, including operating system, email system, migration software and information security software.

16. The estimated \$96.19 million under item (c) above is for acquisition of implementation services for conducting system analysis and design, development, testing, installation, system migration and making training plans. The relevant cost item also includes the services for security risk assessment and audit in various implementation stages.

17. The estimated \$45.81 million under item (d) above is for hiring contract staff who have relevant technical skills and experience to assist in conducting system design, installation, testing and implementation.

18. The estimated \$9.9 million under item (e) above is for other expenditure, including communication network, site preparation, user training, procurement of consumables (e.g. backup tapes) and data centre expenses.

19. The estimated \$22.92 million under item (f) above is for contingency, which is 10% of the sum of items (a) to (e) in paragraph 13.

Recurrent Expenditure

20. The new system will incur an annual recurrent cost of \$13.19 million after its complete rollout in 2021-22, with breakdown as follows -

Item	\$ million
(a) Hardware and Software Maintenance	7.19
(b) System Maintenance	5.25
(c) Others	0.75
Total	13.19

21. The above recurrent cost is for OGCIO to manage, operate, maintain and support CMMP.

22. After implementing CMMP, B/Ds will no longer need to maintain the existing email system of their own. The savings by B/Ds from the hardware, software and system maintenance, as well as technical support resources, are on par with the recurrent cost for managing, operating, maintaining and supporting CMMP by OGCIO. Therefore, there will be no additional recurrent cost for the Government as a whole.

Implementation Plan

23. The estimated schedule for the implementation of CMMP is as follows:

Task	Estimated Schedule
1. Seeking funding approval from the Finance Committee of the Legislative Council	Q2/2017
2. Completion of Tendering	Q3/2017
3. System Development	Q4/2017 to Q4/2018
4. Production Rollout (by phase for B/Ds listed at <u>Annex</u>)	Q4/2018 to Q2/2020

Advice Sought

24. Subject to Members' support of the proposal of implementing CMMP, we will proceed to seek funding approval from the Finance Committee according to the timetable in paragraph 23.

Innovation and Technology Bureau
Office of the Government Chief Information Officer
March 2017

B/Ds which are to implement CMMP¹

1.	Central Policy Unit
2.	Civil Service Bureau
3.	Home Affairs Bureau
4.	Chief Executive's Office
5.	Security Bureau
6.	Department of Justice
7.	Constitutional and Mainland Affairs Bureau
8.	Chief Secretary for Administration's Office
9.	Food and Health Bureau
10.	Financial Secretary's Office
11.	Financial Services and the Treasury Bureau - Financial Services Branch
12.	Financial Services and the Treasury Bureau - Treasury Branch
13.	Commerce and Economic Development Bureau - Communications and Creative Industries Branch
14.	Commerce and Economic Development Bureau - Commerce, Industry and Tourism Branch
15.	Education Bureau
16.	Innovation and Technology Bureau
17.	Innovation and Technology Bureau – Innovation and Technology Commission
18.	Innovation and Technology Bureau – Office of the Government Chief Information Officer
19.	Labour and Welfare Bureau
20.	Development Bureau
21.	Transport and Housing Bureau
22.	Environment Bureau

¹ Listed according to the number of strokes of Chinese characters