HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

24 May 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Cybersecurity Fortification Initiative

I am writing to draw your attention to the Cybersecurity Fortification Initiative (CFI), which is being pursued by the Hong Kong Monetary Authority (HKMA) in collaboration with the banking industry, and to explain our supervisory expectation regarding your institution's adoption and implementation of the initiative.

As explained in our circular of 15 September 2015, the sophistication and potential impact of cyber attacks are on the rise and there is a need for the Board[1] and senior management of authorized institutions (AIs) to play a proactive role in ensuring effective cyber security risk management in their institutions. To further enhance the cyber resilience of the banking sector, the HKMA has been working closely with the banking sector to develop the CFI, which is underpinned by three pillars outlined below (please refer to the **Annex** for further details):

(i) Cyber Resilience Assessment Framework, which is a risk-based framework for AIs to assess their own risk profiles and benchmark the level of defence and resilience that would be required to accord appropriate protection against cyber attacks. The draft framework will be issued shortly to the banking industry for consultation for a period of three months;

(ii) Professional Development Programme, which seeks to increase the supply of qualified professionals in cybersecurity going forward. The HKMA is working with the Hong Kong Applied Science and Technology Research Institute (ASTRI) and the Hong Kong Institute of Bankers (HKIB) on the design structure of the Professional Development Programme, targeting to roll it out by the end of this year; and

[1] For a locally-incorporated AI, the Board may delegate its oversight duties to designated Board-level committee(s). As regards the Hong Kong operations of an overseas incorporated AI, the term "Board" in this circular refers to the local senior management of the AI, under the scrutiny of its head office or regional headquarters.

(iii) Cyber Intelligence Sharing Platform, which provides an effective infrastructure for sharing intelligence on cyber attacks. The timeliness of receiving alerts or warnings from a commonly shared intelligence platform will be of immense help to the banking sector as a whole to prepare for possible cyber attacks. The HKMA, in collaboration with the ASTRI and the Hong Kong Association of Banks (HKAB), is going to launch the platform.

Given the strategic importance of cyber resilience for the banking sector, it is crucial for you to ensure that your institution will adopt and implement the CFI. Specifically, AIs should actively participate in the consultation for the cyber resilience assessment framework. They will be required to carry out the cyber resilience assessment using the framework, unless an equally effective framework is available. Once the risk profile of an AI and the level of resilience needed are established, the Board and the senior management should put in place proper governance arrangements and processes to achieve the level of resilience in cybersecurity commensurate with the risk profile of the AI. The assessment should be conducted by qualified professionals who possess the necessary knowledge and expertise. The HKMA considers IT professionals certified under the Professional Development Programme to be able to satisfy this requirement. In cases where other IT professionals are appointed to conduct the assessment, the management of AIs should satisfy themselves that these professionals possess comparable expertise. In addition, all banks are expected to join the Cyber Intelligence Sharing Platform. To this end, banks should start to make the necessary preparations including system changes at an early stage. The HKMA will set out further details of relevant regulatory requirements related to the implementation of the CFI in due course, taking into account the input of the industry.

Should you have any questions about this circular, please feel free to contact Ms Teresa Chu at 2878 1563 or Mr Tsz-Wai Chiu at 2878 1389. For questions relating to details of the CFI, please approach Mr Josiah Lam at 2878 1425 or Mr Wilson Pang at 2878 1249 of the HKMA's Fintech Facilitation Office directly.

Yours faithfully,

Arthur Yuen
Deputy Chief Executive

Encl.

Annex

HKMA's Cybersecurity Fortification Initiative

To strengthen the cyber resilience of the banking sector in Hong Kong, the HKMA has been working closely with the banking sector to develop the Cybersecurity Fortification Initiative, which is underpinned by three pillars:

I. a Cyber Resilience Assessment Framework;
II. a Professional Development Programme; and
III. a Cyber Intelligence Sharing Platform.

I. Cyber Resilience Assessment Framework

The assessment framework is a tool for assessing an authorized institution (AI)'s cyber risk exposure and cyber resilience. The results will form a basis for an improvement plan of cyber resilience. It also allows the HKMA to get a holistic view of the preparedness of individual AIs as well as the entire banking sector.

The assessment framework will comprise the following three components:

(i) Inherent risk assessment – It is a risk assessment through which AIs are able to assess their cyber risk exposures based on a number of factors, such as the technologies AIs are using for providing services, their usual service delivery channels, products and services offered by AIs, their organizational characteristics, and their track records on defending against cyber attacks. The assessment will result in inherent risk rating of the AIs, i.e. high, medium and low. These inherent risk ratings of AIs are mapped to the respective "required maturity level" of cyber resilience.

(ii) Maturity assessment – It provides a measurable process to assess and determine the "actual maturity level" of AIs, which will be compared with the "required maturity level" of cyber resilience. Any gaps between the "required maturity level" and "actual maturity level" will then be identified for improvement, so that the AI's "actual maturity level" will be brought up to at least the "required maturity level" of cyber resilience.

(iii) intelligence-led cyber attack simulation testing (iCAST) – It is a new intelligence-led cyber attack simulation testing that is to be applied on top of the traditional penetration testing. Simulation test scenarios will be designed to replicate current real life cyber attacks based on specific and up-to-date threat intelligence. AIs, which aim to attain the "intermediate" or "advanced" maturity level, are supposed to execute the cyber attack

simulation test.

II. Professional Development Programme

The HKMA is working with Hong Kong Institute of Bankers (HKIB) and Hong Kong Applied Science and Technology Research Institute (ASTRI) to develop a localized certification scheme and training programme for cybersecurity professionals.

It is an integrated and well-structured programme to train and nurture cybersecurity practitioners in the AIs and the information technology industry, and to enhance their cybersecurity awareness and technical capabilities of conducting cyber resilience assessments and simulation testing.

III. Cyber Intelligence Sharing Platform

Cyber intelligence could be used by AIs to proactively strengthen their cyber resilience posture to better prepare for any potential cyber threats, and to take timely actions to strengthen the preventive, detective and recovery processes.

To help improve the capability of AIs in cyber intelligence sharing and to support the implementation of iCAST, the HKMA is working with Hong Kong Association of Banks (HKAB) and ASTRI to implement a cyber intelligence sharing platform.

Relevant cyber intelligence sourced from different reliable channels will be collected, analyzed and shared on this platform together with detailed cyber-threat analysis report advisories and recommendations. Through this platform, member banks of HKAB will be able to tap the latest threat scenarios and get prepared accordingly.