CONSULTATION PAPER

P014 - 2018

September 2018

NOTICE ON CYBER HYGIENE

Monetary Authority of Singapore

Contents

1 Preface 3

2 DRAFT NOTICE ON CYBER HYGIENE 5

3 Annex A 10

4 Annex B 11

1 Preface

1.1 Technological innovation and advancements are rapidly digitalising and transforming the financial sector. The success of the digital transformation in the financial sector is underpinned by the safety and soundness of these technologies.

1.2 Financial institutions ("FIs") must ensure they have a robust and sound risk management framework to manage the technology and cyber risks. In 2013, MAS updated the Technology Risk Management Guidelines to enhance the guidance to FIs on technology risk management and cyber security practices, and issued a Notice on Technology Risk Management which sets out requirements relating to system recoverability and reliability, incident reporting, as well as protection of customer information respectively.

1.3 In view of the deepening cyber threat landscape and to further strengthen the overall cyber resilience of FIs, MAS intends to issue a Notice on Cyber Hygiene, which prescribes a set of essential cyber security practices that FIs must put in place to manage cyber threats. This is because many of the cyber breaches which occurred globally were often due to poor cyber hygiene.

1.4 In developing the Notice, MAS has referred to the cyber security guidance and regulations in other major jurisdictions to extract the most relevant and effective hygiene practices for FIs to adopt. These measures, if well implemented, would be effective against a wide range of cyber attacks.

1.5 MAS invites interested parties to submit their views and comments on the draft Notice.

Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like (i) their whole submission or part of it, or (ii) their identity, or both, to be kept confidential, please expressly state so in the submission to MAS. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

1.6 Please submit your comments by 5 October 2018 to:

Technology Risk and Payments Department
Technology Risk Supervision
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Fax: 62209659
Email: techrisk@mas.gov.sg

1.7 Electronic submission is encouraged. We would appreciate that you use the prescribed format for your submission to ease our collation efforts.

2 DRAFT NOTICE ON CYBER HYGIENE

MAS NOTICE xxx
Issue Date: xx xxx 2018

IMPLEMENTATION OF CYBER HYGIENE PRACTICES

Introduction

1 This Notice is issued pursuant to section XX of the XXX Act.

Question 1.	MAS seeks views on the proposal to impose requirements on the following entities that are or will be licensed, approved, registered or regulated by MAS (each a "relevant entity"): • any bank licensed under the Banking Act (Cap. 19); • any insurer licensed or regulated under the Insurance Act (Cap. 142); • any insurance intermediary registered or regulated under the Insurance Act; • any person licensed under the Banking Act (Cap. 19) to carry on the business of issuing credit cards or charge cards in Singapore; • any approved holding company, approved exchange, recognised market operator, licensed trade repository, licensed foreign trade repository, approved clearing house, recognised clearing house under the Securities and Futures Act (Cap. 289); • the Depository as defined in section 81SF of the Securities and Futures Act (Cap. 289); • any holder of a capital markets services licence under the Securities and Futures Act (Cap. 289); • any registered fund management company under paragraph 5(1)(i) of the Second Schedule to the Securities and Futures (Licensing and Conduct of Business) Regulations; • any trustee for a collective investment scheme authorised under section 286 of the Securities and Futures Act, that is approved under that Act; • any licensed financial adviser under the Financial Advisers Act (Cap. 110); • any designated payment system operator or settlement institution under the Payment Systems (Oversight) Act (Cap 222A); • any finance company licensed under the Finance Companies Act (Cap. 108); • any designated financial holding company under the Financial Holding Companies Act 2013 (Act 13 of 2013);

- any licensed trust company under the Trust Companies Act (Cap. 336);
- any person that is approved as a financial institution under section 28 of the Monetary Authority of Singapore Act (Cap 186);
- any licensed credit bureau or approved member of a licensed credit bureau[1] under the Credit Bureau Act 2016 (Act 27 of 2016);
- any licensee under the proposed Payment Services Bill[2] (this will include existing money changers, remittance agents and holders of stored value facilities that become licensees under the proposed Payment Services Bill; as well as proposed payment services such as account issuance, domestic money transfer, merchant acquisition and virtual currency services); and
- any authorised benchmark administrator, authorised benchmark submitter or designated benchmark submitter under the Securities and Futures Act (Cap. 289) as amended by the Securities and Futures (Amendment) Act 2017 (Act 4 of 2017).

Definitions

2 For the purpose of this Notice----

"administrative account", in relation to a system, means any user account that has full privileges and unrestricted access to the system;

"confidential information" means —

(a) any information relating to, or any particulars of, any customer of the relevant entity that is not publicly available; and

(b) any information relating or belonging to the relevant entity that is not publicly available;

[1] The Credit Bureau Act has been passed in Parliament and is pending commencement. The Second Reading and explanatory brief of the Credit Bureau Bill can be found at http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Credit-Bureau-Bill-2016.aspx and http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/Explanatory-Brief-Credit-Bureau-Bill-2016.aspx.

[2] While the public consultation has closed, you may refer to the paper for details of the proposed Payment Services Bill: http://www.mas.gov.sg/News-and-Publications/Consultation-Paper/2017/Consultation-Paper-on-Proposed-Payment-Services-Bill.aspx.

"critical system" in relation to a relevant entity, means a system, the failure of which will cause significant disruption to the operations of the relevant entity or materially impact the relevant entity's service to its customers. A critical system includes but is not limited to a system which —

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"multi-factor authentication" means the use of two or more factors to verify an account holder's claimed identity. Such factors include, but are not limited to:—
(a) something that the account holder knows such as a password or a personal identification number;
(b) something that the account holder has such as a cryptographic identification device or token;
(c) something that the account holder is such as an account holder's biometrics or his behaviour;

"security patch", in relation to a system, means an update that can be applied to the system to address a vulnerability;

"security standards", in relation to a system, means a set of configurations and procedures for the purpose of safeguarding and improving the security of the system;

"system", in relation to a relevant entity, means any hardware, software, network, or other information technology ("IT") component used by the relevant entity;

"vulnerability", in relation to a system, means any weakness, susceptibility or flaw of the system that can be exploited, including but not limited to by allowing an unauthorised person to access the system, or to compromise the security configuration settings of the system.

3 Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires, have the same meaning as in the Act.

Question 2.	MAS seeks comments on the proposed definitions to be used in the Notice, in particular, whether they are sufficiently clear and suitable. If you propose a different definition for the same term that is from another legislation or paper, please cite the full title of the legislation or paper and the specific provision in that legislation or paper where the term is defined.

Cyber Hygiene Practices

4 **Administrative Accounts**: A relevant entity must secure every administrative account on its system to prevent any unauthorised access to or use of, such account.

5 **Security Patches**:

(a) A relevant entity must apply security patches to address vulnerabilities to its system, within a timeframe that is commensurate with the risks posed by such vulnerabilities being exploited to the relevant entity.

(b) Where no security patch is available to address a vulnerability, the relevant entity must institute controls to reduce any risk posed by such vulnerability to its system.

6 **Security Standards**:

(a) A relevant entity must have a written set of security standards for its system.

(b) Subject to sub-paragraph (c), a relevant entity must ensure that its system conform to the set of security standards.

(c) Where the system is unable to conform to the set of security standards, the relevant entity must institute controls to reduce any risk posed by such non-conformity.

7 **Firewall**: A relevant entity must implement one or more firewalls at its network perimeter to restrict all unauthorised network traffic.

8 **Anti-virus**: A relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system.

9 **Multi-factor Authentication:** A relevant entity must implement multi-factor authentication for the following:

(a) all administrative accounts on its critical system; and

(b) all accounts on any system used by the relevant entity to access confidential information through the internet.

Question 3. MAS seeks comments on the cyber security requirements and whether there are other security controls and processes which should be included in the Notice to supplement the above. A non-exhaustive list of measures that can be implemented by the relevant entity to meet the requirements in this Notice are set out in Annex B.

Effective Date

10 This Notice shall take effect from XX.

Question 4. The effective date will be 12 months from date of issuance of the Notice. MAS seeks comments on whether the transition period is adequate for the financial institutions to implement the frameworks, processes and controls to comply with the requirements.

3 Annex A

LIST OF QUESTIONS

Question 1. MAS seeks views on the proposal to impose requirements on the following entities that are or will be licensed, approved, registered or regulated by MAS (each a "relevant entity"): 5

Question 2. MAS seeks comments on the proposed definitions to be used in the Notice, in particular whether they are sufficiently clear and suitable. If you propose a different definition for the same term that is from another legislation or paper, please cite the full title of the legislation or paper and the specific provision in that legislation or paper where the term is defined. 7

Question 3. MAS seeks comments on the cyber security requirements and whether there are other security controls and processes which should be included in the Notice to supplement the above. A non-exhaustive list of measures that can be implemented by the relevant entity to meet the requirements in this Notice are set out in Annex 8

Question 4. The effective date will be 12 months from date of issuance of the Notice. MAS seeks comments on whether the transition period is adequate for the financial institutions to implement the frameworks, processes and controls to comply with the requirements. 9

4 Annex B

GUIDANCE TO COMPLY WITH CYBER HYGIENE REQUIREMENTS

The table below contains measures that can be implemented by a relevant entity to meet the requirements stipulated in the Notice. Due to the differences in the scale, complexity and nature of business of different entities, the measures that a relevant entity must implement to comply with this Notice may differ from that implemented by another relevant entity.

Cyber Hygiene Requirements	Measures
Para 4 - Administrative Accounts	• Keep a record all administrative accounts in its system. • Implement strong password controls such as changing the default password, enforcing minimum password length and password complexity. • Grant access to administrative accounts only to authorised staff. • Validate on a regular basis that only authorised persons have access to administrative accounts.
Para 5 - Security Patch	• Perform regular checks for available security patches. • Establish a framework to assess the criticality of any available patch and the timeframe within which the patch must be implemented. • The framework should include controls to reduce any risk in the event that a patch cannot be applied.
Para 6 - Security Standards	• Establish, document and keep up-to-date security standards. • Ensure every system complies with the security standards established by the relevant entity. • Take steps to reduce any risk, including approving deviations from the security standards, if the system cannot fully conform with the security standards.
Para 7 - Firewall	• Implement one or more firewalls at the network perimeter in order to segment the internal network from the public internet. • Configure any implemented firewalls and regularly review the firewall rules to only allow authorised network traffic to pass through.
Para 8 - Anti-virus	• Update any anti-virus software and signatures promptly.
Para 9 - Multi-factor Authentication	Implement multi-factor authentication for the accounts as stated in the Notice. Examples include but are not limited to: • any administrative account of an operating system on any critical system; • an account belonging to Human Resource Department that can be used to remotely access staff information through the internet.

Monetary Authority of Singapore