RESPONSE TO FEEDBACK RECEIVED

6 August 2019

DRAFT NOTICE ON CYBER HYGIENE

MAS

Monetary Authority of Singapore

Contents

1 Preface 3

2 Applicability 3

3 General comments on the requirements 5

4 Definitions 7

5 Administrative Accounts 7

6 Security Patches 8

7 Security Standards 8

8 Firewall 9

9 Anti-virus 11

10 Multi-Factor Authentication 12

11 Effective Date of the Notice 14

Annex A List of Respondents to the Consultation Paper 15

Annex B Submissions to the Public Consultation 19

1 Preface

1.1 On 6 September 2018, MAS issued a Consultation Paper on Notice on Cyber Hygiene (“the Notice”) which sets out fundamental cybersecurity best practices that were elevated from the Technology Risk Management Guidelines (“TRMG”) into legally binding requirements. Given the persistent and evolving nature of cyber threats, financial institutions or relevant entities must implement these requirements to secure and to protect their IT systems from cyber-attacks. The consultation period closed on 5 October 2018.

1.2 MAS would like to thank all respondents for their feedback and comments. MAS’ responses to the feedback and comments are set out in the subsequent paragraphs. Unless specifically requested for confidentiality, the respondents’ identities and their submissions are provided in Annex A and Annex B respectively.

1.3 The finalised Notice on Cyber Hygiene is published on the MAS website. The Notice will come into effect on 6 August 2020.

2 Applicability

Registered Fund Management Company

2.1 A registered fund management company (“RFMC”) commented that it has existing practices to prevent theft of information and highlighted that the requirements in the Notice will increase compliance costs with little or no improvement to RFMCs’ cybersecurity.

MAS’ Response

2.2 Cyber-attacks present a clear and substantial threat to the financial sector. Every financial institution (FI), or a relevant entity, must strengthen its cyber resilience to guard against such threats. The Notice prescribes a set of fundamental cyber security requirements that are effective in mitigating prevalent cyber threats. It is of paramount importance that all relevant entities secure their IT systems according to the requirements set out in the Notice.

2.3 As the use of technology solutions and the scale of IT operations varies across the relevant entities, MAS will not specify the measures that relevant entities must implement to meet the requirements. The relevant entities must assess whether their current measures are able to meet the requirements in the Notice and put in place the appropriate measures to ensure full compliance with the Notice. These measures can take the form of process and operational controls, or implementation of technology solutions.

Insurance Agents, Exempt Financial Advisers, Representatives of Licensed Financial Advisers and of Exempt Financial Advisers

2.4 Respondents sought to confirm whether the Notice will be applicable to exempt financial advisers, insurance agents and representatives of licensed financial advisers and of exempt financial advisers. Respondents also highlighted that representatives will not be able to meet the requirements of the Notice and sought to understand the liability of financial advisers for its representatives in the event of a breach.

MAS' Response

2.5 The Notice is **not** issued to:

(a) **exempt financial advisers**[1]; and

(b) representatives of financial advisers and **individuals** who are insurance agents.

2.6 While MAS regulates representatives, we will not impose the requirements on them but will impose the requirements at the entity level, i.e. on the licensed financial adviser.

Foreign-incorporated recognised market operators (RMOs), foreign-incorporated recognised clearing houses (RCHs) and licensed foreign trade repositories (LFTRs)

2.7 Respondents opined that foreign-incorporated RMOs, foreign-incorporated RCHs and LFTRs should not be subject to the Notice as these entities are primarily regulated by their home regulator.

MAS' Response

2.8 MAS will not issue the Notice to the foreign-incorporated RMOs, foreign-incorporated RCHs, and LFTRs. Most of the activities of foreign-incorporated RMOs, foreign-incorporated RCHs, and LFTRs are not performed in Singapore and MAS would have satisfied itself that the regulatory regime in the home jurisdiction of the entity achieves comparable outcomes as the regulatory regime in Singapore, and that there are adequate arrangements for cooperation with the home regulator of the entity on information exchange and mutual assistance. On this basis, MAS exercises a less intrusive approach towards the supervision of such entities.

[1] However, please note that exempt financial advisers who are otherwise licensed by MAS e.g. as a capital markets services license holder or a bank will be subject to the Notice.

Entities under the proposed Payment Services Bill ("PSB")

2.9 Respondents highlighted that the proposed PSB had not been finalised (at the time of public consultation) and requested MAS to defer the decision to apply the Notice to the proposed list of entities that will be licensed under the PSB. Some respondents highlighted that they should not be subject to the Notice as they would need to comply with the requirements under the Cyber Security Act.

MAS' Response

2.10 The PSB was passed in Parliament in January 2019 and the Payment Services Act 2019 ("PS Act PSA") was published in 22 February 2019. MAS will issue the Notice to licensees and operators of designated payment systems under the PS Act and the Notice will take effect on 6 August 2020.

2.11 The Notice sets out a minimum set of cybersecurity measures that is aimed at protecting relevant entities' systems from cyber-attacks. While relevant entities are required to comply with the specific requirements in the Notice, they should also ensure they meet the other relevant legal and regulatory requirements that they are subject to.

Enforcement and Penalty for Non-Compliance

2.12 A few respondents requested to understand the penalty and enforcement actions for non-compliance with the Notice.

MAS' Response

2.13 The Notice will be issued under the provisions of the various statutes which MAS administers. Relevant entities can refer to the specific provisions under the statutes which they are regulated to better understand the penalties. For example, if the Notice is issued to banks under section 55(1) of the Banking Act, the penalty for non-compliance is provided for in section 71 of the Banking Act. MAS, in determining the enforcement actions in the event of a breach of the Notice, will assess the extent to which the relevant entity had implemented the necessary measures to meet the requirements of the Notice.

3 General comments on the requirements

Risk-based approach

3.1 Some respondents asked for prescriptive measures to help the relevant entities meet the requirements in the Notice. Respondents highlighted that the scope of systems described in the Notice is too all-encompassing and requested that the relevant entities should be allowed to adopt a risk-based approach in determining the scope of systems. For example, the scope can be limited to critical systems, systems used by the relevant entity to process customer information, and devices that provide a potential entry point into the entity's internal network.

MAS' Response

3.2 As the Notice applies to relevant entities of varying size and complexity, prescribing specific measures, such as review frequency or a set of system parameters will not be practical. Therefore, relevant entities are expected to have in place a proper IT risk management framework to facilitate the assessment of risks, and they must implement the appropriate measures to mitigate those risks to comply with the Notice.

3.3 The intent of the Notice is to mandate protect the systems used by the relevant entity, by setting out a set of fundamental cybersecurity requirements. Systems with weak security are vulnerable to cyber-attacks, and can serve as a potential entry points into the network for hackers.

Outsourcing and Third Party

3.4 Respondents sought clarifications on the applicability of the Notice to third parties, including intragroup or outsourced service providers, where the responsibilities for cyber security policies, processes and systems are established and owned by third parties and are outside the control of the relevant entity.

MAS' response

3.5 MAS views systems provided by third parties as "systems within the control of the entity" because relevant entities are able to impose terms and conditions in their contractual agreements with the third parties to ensure the systems implemented or used by the relevant entities meet the requirements set out in the Notice.

Differences between the Notice and the Technology Risk Management Notice

3.6 Respondents sought clarifications from MAS on differences between the Notice and the Notice on Technology Risk Management ("TRMN").

MAS' Response

3.7 The Notice requires relevant entities to implement a set of cybersecurity measures to protect and secure their systems from cyber-attacks. The TRMN, on the other hand, sets out requirements for FIs to maintain a high level of availability and recoverability in their critical systems, protect customer information from unauthorised access or disclosure, and to report relevant incidents to MAS.

4 Definitions

4.1 Respondents suggested that the common definitions used in both Notices, specifically for “critical systems” and “systems”, should be aligned.

MAS’ Response

4.2 MAS has aligned the definition of critical systems in the Notice with that of the Technology Risk Management Notice.

5 Administrative Accounts

Types of administrative accounts

5.1 Respondents sought clarifications on the extent of privileges and the access that these administrative accounts have and whether non-user administrative accounts are also subject to the requirement.

MAS’ Response

5.2 The administrative accounts, as defined in the Notice, are user accounts that have full access rights (i.e. read, write and execute) to key system resources.

5.3 MAS has also revised the definition of “administrative accounts” to those accounts on the operating systems, databases, applications, security appliances and network devices that are used by and within the control of the relevant entities. Non-user held or non-interactive administrative accounts, such as service accounts or system accounts, used by operating systems to run services are excluded from the Notice.

Measures required to secure administrative accounts

5.4 Some respondents requested MAS to prescribe minimum standards in areas, such as password control, frequency to review access to administrative accounts. Respondents also suggested to incorporate additional measures in the requirement to secure administrative accounts such as setting maximum validity period and segregate duties for granting and approving the use of administrative accounts.

MAS’ Response

5.5 MAS has shared some of the common industry practices in an FAQ that will be issued together with the Notice to guide relevant entities on securing the administrative accounts on their systems.

6 Security Patches

Risk-based approach

6.1 Many respondents highlighted challenges in ensuring all systems are patched within a timeframe and proposed a risk-based requirement to allow relevant entities to determine whether to apply and prioritise a patch based on system criticality, severity of the vulnerability or risks posed by the vulnerability.

MAS' Response

6.2 The requirement in the Notice allows the relevant entity to adopt a risk-based approach when determining the timeframe to deploy the patches, taking into consideration the security severity of the patches, criticality of the affected systems, risks associated with the vulnerabilities that the patches are supposed to address and the existing controls in its IT environment.

Risk of applying security patches and other mitigating controls

6.3 Many respondents highlighted that the patching may break the systems if the patch is not compatible. Some respondents sought clarifications on the mitigation controls that are acceptable if security patches cannot be applied because they are incompatible, or if patches are not available.

MAS' Response

6.4 MAS acknowledged respondents' concerns that some patches could disrupt the relevant entity's operations due to incompatibility between the patch and the system.

6.5 In the event that a patch cannot be applied or is not available, relevant entities shall perform a risk assessment and consider appropriate risk mitigating measures to address the risks associated with the vulnerabilities that the patch is intended to resolve. MAS has shared common industry practices within the FAQ.

7 Security Standards

Scope and types of security standards

7.1 Many respondents requested MAS to provide examples of security standards. Some respondents asked whether security standards would include controls, such as the management of system access rights, system monitoring, source code review and penetration testing. A few respondents suggested removing the term "procedures" from the definition so it is clear that the standards refer to only technical controls.

MAS' Response

7.2 Based on feedback from respondents, MAS has removed the term "procedures" from the definition of "security standards" to better reflect MAS' intention for its scope to cover technical controls.

7.3 Relevant entities may refer to internationally recognised industry best practices such as Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) when formulating their security configurations standards to harden or to improve the security of their systems.

Approval and frequency of review of the standards

7.4 Respondents sought clarification on who should be the appropriate personnel in the relevant entity to approve the security standards, and the frequency to review security standards.

MAS' Response

7.5 A relevant entity should ensure the security standards are approved by the person who has oversight responsibilities over the cybersecurity function. The relevant entity should review and update its standards at least yearly, or whenever there are significant changes to its IT environment or to the cyber risk landscape.

Security standards for devices

7.6 Some respondents also highlighted that CCTV, projectors, printers and Internet-of-Things devices may not have industry security standards.

MAS' Response

7.7 Industry security standards are formulated based on well-established security principles (e.g. least privilege, separation of duties, defence-in-depth, etc.) and objectives (e.g. to maintain confidentiality, integrity and availability). While relevant entities should, as far as possible, adopt available industry security standards to govern the configuration of devices deployed in their organisation, it could be the case that there are no industry standards available for certain types of devices. In this regard, relevant entities could examine the settings and configurations available on the devices, and identify the security principles and objectives that would be applicable to establish their organisational security standards for those devices.

8 Firewall

Security devices with firewall capabilities

8.1 Some respondents suggested the use of a broader term to protect network perimeters given that firewall is only one type of security devices that could be used to secure the internal network. Respondents sought clarity on whether it was a requirement to implement perimeter monitoring or network intrusion detection capability as set out in Circular No. SRD TR 01/2015 on Early Detection of Cyber Intrusion. One respondent suggested that MAS defines the frequency to review firewall rules.

MAS' Response

8.2 MAS noted the feedback that there are other security devices that have capabilities similar to firewalls to protect network perimeters. MAS has revised the requirement to allow relevant entities to exercise flexibility in choosing the device to implement to protect its network from unauthorised traffic. Network intrusion detection capability is not a requirement in the Notice.

8.3 The review frequency should commensurate with factors, such as the criticality of systems in the network and the level of cyber risks. In this regard, MAS will not be prescribing the frequency as the aforementioned factors are unique for different IT environments.

Scope of network

8.4 Respondents queried how the requirement should be applied to a network that is outsourced to intra-group or third party service providers. Some respondents also asked whether the requirement to implement firewalls applies for an entity with less than five computers.

MAS' Response

8.5 The requirement in the Notice will apply to all networks used by relevant entities, including those hosted overseas, outsourced to intra-group or to third party service providers. To meet the requirement, a relevant entity is required to implement measures that are commensurate with the scale and complexity of its networks. Examples of possible solutions would include implementing network router or firewall.

Internet Surfing Separation

8.6 One respondent asked whether MAS is expecting relevant entities to implement internet surfing separation (ISS).

MAS' Response

8.7 ISS is not a requirement in the Notice.

9 Anti-virus

Malware Protection Measures

9.1 Respondents suggested to replace "virus" with "malware" as the latter is a broader term which includes all types of malicious software. A few respondents highlighted that the prevention of malware infection may involve other measures, such as threat detection and response solutions, and suggested that the relevant entities be allowed to decide on the measures to be implemented.

<u>MAS' Response</u>

9.2 MAS noted the industry's feedback and has replaced "anti-virus" with "malware protection" to better reflect the intent of the requirement. Before implementing malware protection measure, relevant entities should perform their own risk assessment to determine if other measures are required to enhance their capability to mitigate the threat of malware infection on their systems.

Applicability of Malware Protection Solutions

9.3 Respondents indicated that there could be issues arising from installation of anti-malware solutions on systems and these issues could range from an increased risk of service unavailability and degradation in database performance. Some respondents also highlighted that anti-malware solutions might not be available for some operating systems such as Unix.

<u>MAS' Response</u>

9.4 Given the diverse range of malware protection products available in the market, relevant entities could work with the vendors to identify the most suitable malware protection solution that meets their own needs and the Notice requirements. In circumstances where malware protection solutions are not available for a particular platform, relevant entities do not need to implement anti-malware protection measures.

Additional Measure

9.5 Respondents highlighted that a single malware protection solution may be inadequate to provide protection in light of the sophistication and the polymorphic nature of malware and recommended that MAS consider the need for entities to implement defence-in-depth measures to detect and prevent malware infection.

<u>MAS' Response</u>

9.6 MAS' intent is for relevant entities to put in place a set of the cybersecurity measures to protect against the most common cyber attacks. Notwithstanding this, the Notice should not preclude relevant entities from implementing additional measures to further mitigate the risk of malware infection or cyber attacks on their systems.

10 Multi-Factor Authentication

Definition of confidential Information

10.1 Respondents highlighted that the definition of confidential information used in the Notice could include almost all information within the organisation (i.e. those not publicly available), including those held by third parties but belonging to the organisation. To subject accounts that can access such information to multi-factor authentication would be overly restrictive for businesses. Respondents suggested that confidential information should be restricted to information, such as those that is commercially sensitive or employee information. Some respondents also suggested to align with the definition used in the MAS' Outsourcing Guidelines.

MAS' Response

10.2 MAS noted the industry feedback and will only require relevant entities to protect their customer information. The definition of customer information has been revised accordingly to mean any information relating to, or any particulars of, any customer of the relevant entity where a named customer or group of named customers can be identified, or is capable of being identified, from such information.

Scope of application for MFA

10.3 Respondents sought to clarify whether multi-factor authentication (MFA) must be implemented for system-to-system communications and for their customers. Other respondents enquired whether MFA is required to access systems that are connected over leased lines and through Virtual Private Network (VPN).

MAS' Response

10.4 The definition of administrative accounts does not include non-user or non-interactive administrative accounts. User accounts held or used by the relevant entities' customers, such as internet or online banking, are not in the scope of the Notice.

10.5 The MFA requirement applies to accessing administrative accounts on critical systems, regardless of the access channel (e.g. leased line or VPN). For accessing customer information over the internet, relevant entities should determine how to implement MFA e.g. at the VPN server or at the application to authenticate the users.

Authentication Factors

10.6 Respondents asked if One-Time-Password ("OTP") via the short-message-service ("SMS") or a software token application could be used as one of the factors. Some respondents enquired on whether MFA would apply to accessing emails via mobile phones and suggested that the device identity should be included as one of the MFA factor. Respondents also enquired whether the use of step-up authentication[2] or the use of a centralised password vault meets the MFA requirement.

MAS' Response

10.7 To fulfil the MFA requirement, two or more unique and independent authentication factors must be implemented. Examples of authentication factors include One-Time Password (OTP) generated from a hardware or software token or delivered through SMS, biometrics, unique device identity, digital certificate, or password.

10.8 The definition of MFA has been revised to include device identity and digital certificate as an authentication factor. However, relevant entities should ensure device identity should be bound securely[3] to the user account, if device identity is to be used as a unique factor.

10.9 Step-up authentication will meet the MFA requirement, as long as there is another separate factor to authenticate users before they are allowed to access more sensitive information or to perform higher risk activities. The use of a centralised password management tool will not fulfil the requirement of MFA if the authentication to the critical system relies on only one factor.

Unable to support MFA

10.10 Respondents highlighted that some legacy systems may not have built-in support for MFA, or may encounter stability issues when integrated with MFA solutions.

MAS' Response

10.11 MAS noted the potential challenges in the implementation of MFA on legacy systems. Relevant entities could utilise a third-party software application or appliance to implement MFA to control access to their legacy systems.

[2] Step-up authentication involves the use of stronger authentication mechanism or separate factors to allow a user to access more sensitive information or to perform higher risk activities.

[3] A stringent process must be in place to tie a user to a device, such as through an authentication process.

11 Effective Date of the Notice

11.1 While most respondents agreed with the 12-month minimum period for relevant entities to comply with the Notice, some highlighted that they might not be able to implement all the requirements. Some of the respondents requested for MAS to extend the period to 18 or 24 months, in particular, for the MFA requirement as relevant entities might need time to source for appropriate solutions or to engage external parties to help to study the existing IT infrastructure and implement the necessary controls.

11.2 Respondents also requested for MAS to consider a framework to address non-compliance during the time period after the Notice is effective but relevant entities are in the process of implementing the requirements.

MAS' Response

11.3 MAS is of the view that the requirements in the Notice are not new and relevant entities should already have these fundamental cybersecurity measures in place. Hence, a 12-month transition period is adequate for relevant entities to achieve compliance. For the requirement on multi-factor authentication, relevant entities have until 5 February 2021 to comply, subject to the fulfilment of specific conditions set out in the Notice.

11.4 MAS will assess the relevant entities' extent of compliance with the Notice during the course of its supervision of the entities. The relevant entity has to show cause of extenuating circumstances for not being able to comply within the stated timeframe.

Annex A List of Respondents to the Consultation Paper

A total of 123 submissions were received of which 17 respondents requested confidentiality of their identity, 3 respondents requested confidentiality of their submission and 31 respondents requested confidentiality of both their identity and submission.

**Respondents who requested confidentiality of their identity*
#Respondents who requested confidentiality for their submitted response

1. F12 DATA PTE LTD
2. An individual*
3. Edge Insurance Brokers (Singapore) Pte Ltd
4. Wang Mengran
5. Network Intelligence Pte. Ltd.
6. Econopolis Singapore Pte Ltd
7. Lighthouse Advisors Private Limited
8. Trendlab Pte. Ltd.
9. iTGRC Security and Compliance group, Cyber Advisory Services, CHK Consulting
10. Prusik Investment Management Singapore Pte. Ltd
11. Detack GmbH
12. An entity*#
13. CME Group Inc.
14. An entity*#
15. Fullerton Fund Management Company Ltd
16. SINGAPORE POST LIMITED
17. An individual*
18. An entity*#
19. An entity*#
20. An entity*#
21. Lloyd’s of London (Asia) Pte Ltd
22. Tan Hwee Cher
23. An individual*
24. Fidelity International
25. Asia Pacific Exchange Pte. Ltd. and Asia Pacific Clear Pte. Ltd. (collectively referred to as “APEX”)
26. An entity*#
27. Transamerica Life (Bermuda) Ltd
28. An entity*#
29. HSH Nordbank Singapore Branch
30. ABN AMRO Bank N.V., Singapore Branch
31. An entity*#
32. Arab Banking Corporation (B.S.C.), Singapore Branch
33. Association of Independent Asset Managers Singapore (AIAM)
34. A submission comprising of
    i. LIA,
    ii. AIA,
    iii. China Taiping,

iv. Etiqa,
v. Manulife,
vi. NTUC Income,
vii. Tokio Marine Life,
viii. Transamerica Life,
ix. Zurich Int’l Life
x. China Life,
xi. Friends Provident,
xii. Generali,
xiii. Life Insurance Corporation,
xiv. Old Mutual Int’l,
xv. Singapore Life,
xvi. St James’s Place,
xvii. Swiss Life,
xviii. Gen Re,
xix. Munich Re,
xx. Pacific Life Re,
xxi. Partner Re,
xxii. SCOR Global Life and
xxiii. Swiss Re

35. Maybank Singapore#
36. An entity*
37. Rabobank Singapore Branch
38. An entity*#
39. SWIFT
40. The Great Eastern Life Assurance Company Limited
41. An entity*#
42. An entity*
43. ICICI Bank Limited Singapore Branch#
44. Securities Association of Singapore#
45. Forcepoint Overseas Limited
46. MSIG Insurance (Singapore) Pte. Ltd
47. Prudential Assurance Company Singapore (Pte) Ltd
48. An entity*
49. An entity*
50. An entity*#
51. Gartner Advisory Singapore Pte. Ltd
52. An entity*#
53. An entity*#
54. Oracle
55. finexis Asset Management Pte. Ltd.
56. HITRUST Alliance (“HITRUST”)
57. An entity*#
58. "SingCash Pte Ltd Telecom Equipment Pte Ltd Collectively known as “Singtel”
59. St. James’s Place International plc (Singapore Branch) & St. James’s Place (Singapore) Private Limited
60. An entity*#

61. Schroder Investment Management (Singapore) Ltd
62. Insmart Insurance
63. Allianz Global Investors Singapore
64. DP Credit Bureau Pte. Ltd.
65. An entity*#
66. An entity*#
67. Aetna Brokers
68. Control Risks
69. AL WEALTH PARTNERS PTE LTD
70. An entity*#
71. Gemalto, Enterprise & Cybersecurity BU
72. Stradegi Consulting Pte. Ltd.
73. An entity*
74. VISA
75. Industrial & Commercial Bank of China Limited
76. An entity*#
77. An entity*#
78. RHT Compliance Solutions
79. An individual*
80. A submission from Aon Singapore Pte Ltd, Aon Benfield Asia Pte Ltd, Aon Hewitt Wealth Management Pte Ltd, Aon Singapore (Broking Centre) Pte Ltd
81. An entity*
82. An entity*
83. An entity*
84. An entity*#
85. An entity*#
86. CyberArk Software (Singapore) Pte Ltd
87. An entity*#
88. An entity*#
89. Tokio Marine Life Insurance Singapore Ltd.
90. An entity*#
91. Lombard International Singapore Pte. Ltd
92. BNP Paribas Singapore Branch
93. An entity*
94. Funding Societies
95. Direct Asia Insurance (Singapore) Pte Ltd
96. PricewaterhouseCoopers Risk Services Pte. Ltd.
97. Mizuho Bank Ltd., Singapore Branch
98. Aviva Ltd
99. An entity*
100. Investment Management Association of Singapores
101. Network for Electronic Transfers (Singapore) Pte Ltd#
102. EmiratesNBD
103. An entity*#
104. KPMG Services Pte Ltd
105. Hannover Rück SE
106. FWD Singapore Pte. Ltd

107. Legg Mason Asset Management Singapore Pte. Limited
108. An entity*#
109. SGX
110. Unicorn Financial Solutions Pte Limited
111. State Bank of India
112. An entity*
113. MUFG Bank, Ltd.
114. An entity*#
115. An entity*#
116. An entity*
117. Leon Tham
118. An entity*#
119. An entity*#
120. World Federation of Exchanges (WFE)
121. MUFG (Securities) Asia (Singapore)
122. Microsoft Operations Pte Ltd.
123. CREST GB Ltd

Please refer to Annex B for the submissions.

Annex B Submissions to the Public Consultation

SUBMISSIONS FROM RESPONDENTS TO THE CONSULTATION PAPER ON NOTICE ON CYBER HYGIENE

Note: This table below only includes submissions for which respondents did not request confidentiality of submissions.

S/N	Respondent	Feedback from respondent
1.	F12 Data Pte Ltd	**1. Comments on the applicability of the Notice:** No Comments. **2. Comments on the proposed definitions:** No Comments. **3. Comments on the proposed cyber security requirements:** Para 4 – Administrative Accounts • Administrative accounts similar to user's account should have maximum validity period and change password to these account periodically (Technology Risk Guidelines 11.1.5) • Removal of staff accounts that left the organisation within stipulated timeframe in accordance with the security standard set by the entity Wireless Network • Implementing new wireless security protocol that supports stronger cryptography and stronger authentication control • Integrating authentication to wireless network without requiring users to enter the wireless key in prevention of staff sharing wireless network key with external parties • Guest wireless should be considered external network and should pass through the firewall rules for filtering USB storage controls • Only authorised USB storage devices are allowed to be used in the network • Monitor and track information exchanges between the system and USB devices • Disable the use of USB storage devices on all critical systems External application or services • External application or systems (eg: Reuters and Bloomberg terminals, biometric door access should be segregated from the internal network) Document storage / File servers • Periodically review the access rights to files and folders.

S/N	Respondent	Feedback from respondent
		• Disable sharing of files and folders on end user's system to prevent accidental leak of confidential information. **4. Comments on the proposed transition period:** No Comments. **5. General Comments:** No Comments.
2.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
3.	Edge Insurance Brokers (Singapore) Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
4.	Wang Mengran	**1. Comments on the applicability of the Notice:** No Comments. **2. Comments on the proposed definitions:** No Comments. **3. Comments on the proposed cyber security requirements**: It is important to include a requirement for secure transmission of data over open, public network including the Internet. For example, by enforcing HTTPS for web application instead of

S/N	Respondent	Feedback from respondent
		HTTP, the FIs can prevent attacks including (a) Man-in-the-Middle (MiTM) attacks (b) the interception of sensitive personal information from compromised network encryption. This a widely adopted industry best practice internationally. For example, the Payment Card Industry Data Security Standard (PCI-DSS), v3.2.1 – Requirement 4.1 requires all entities involved in payment card processing to "use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks". The free services like Let's Encrypt and Cloudflare's Universal SSL have made encryption over the web (HTTPS) accessible to even the small and medium enterprises (SMEs). **4. Comments on the proposed transition period:** No Comments. **5. General Comments:** No Comments.
5.	Network Intelligence Institute of Information Security	**1. Comments on the applicability of the Notice:** No Comments**.** **2. Comments on the proposed definitions:** No Comments**.** **3. Comments on the proposed cyber security requirements:** In the section on Administrative Accounts. The definition of these accounts should be expanded to include "service" accounts. Often these accounts may have significantly high privileges on the system (but may not be classified as administrative accounts). As these service accounts are used by software that runs on the systems, their passwords don't get changed. And in many lateral movement attacks we see that these accounts are being exploited. On the MFA requirement – service accounts will have to be excluded. One of the key hygiene elements that many organizations miss is imposing password policies uniformly across all systems and accounts. This may be added to the list of requirements. Another key hygiene element that often gets missed out is the people aspect. So, some level of security awareness training

S/N	Respondent	Feedback from respondent
		must be made mandatory for all employees and they must undergo this on at least an annual basis. Security testing – at least all Internet facing systems must undergo a security assessment on an annual basis. Logs – all transaction logs must be maintained. Often, we find that fraud or cybercrime investigations are severely impeded due to a lack of sufficient logs. In line with PCI DSS, a 1-year or at least 6-month log retention period may be mandated. While for smaller financial institutions log monitoring may not be feasible, but possibly generating and storing logs should be strongly considered. **4. Comments on the proposed transition period:** No Comments. **5. General Comments:** Good initiative to raise the bar across the board.
6.	Econopolis Singapore Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
7.	Lighthouse Advisors Private Limited	**1. Comments on the applicability of the Notice:** For Fund Managers the meaningful cyber hygiene risks are: 1. Theft of customer funds/confidential client information 2. Theft of fund manager funds/confidential fund manager information Theft of customer funds is already safeguarded by existing practices in place at the custodian and fund administrator. Theft of confidential customer information is already safeguarded by existing practices in place at the fund administrator. In the case of managed accounts the fund manager is already expected to store the information in a secure place i.e. password protected, not accessible to the public etc.

S/N	Respondent	Feedback from respondent
		Theft of fund manager funds/confidential fund manager information is already safeguarded by existing practices i.e. limited cheque signatories, storage of information in a secure place etc. Requiring Fund Managers to comply with the Notice will increase costs with little or no improvement to security for customers and the fund managers. In particular, for Registered Fund Management Companies, which tend to be smaller in scale and have a limited customer base, the potential damage from a hacking incident is limited, while the compliance costs would be substantial. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Most Fund Managers rely on commercial off-the-shelf software for their work. This means that the computers run Microsoft Windows, Microsoft Office etc. Information is stored in Microsoft Word or Excel documents. They may use commercial services such as Bloomberg Professional, Standard & Poor's, or Thomson Reuters. Information may be stored online with any or all of these services. None of the products from Microsoft, Bloomberg, Standard & Poor's or Thomson Reuters offer multi-factor authentication. As a practical matter, it is impossible to obtain substitutes for the above software and services that can be secured by multi-factor authentication. This means strict compliance would require the Fund Managers to purchase additional software and hardware to secure access to the computers running such commercial software. This is extremely costly and redundant. As a compromise I suggest that (i) any systems that host confidential information must be password-protected and not accessible to the public; and (ii) any files that contain confidential information must be password-protected and not accessible to the public. This effectively creates a 2-password authentication at the system level: one to log onto the computer system, and one to access the file in question. **4. Comments on the proposed transition period:** With regards to #3 above, if Fund Managers are required to implement multi-factor authentication using additional software/hardware, at least 24 months will likely be needed in order to source (or if necessary, self-develop) such software and

S/N	Respondent	Feedback from respondent
		hardware. If 2 levels of password (system/file) are considered sufficient, 12 months is a sufficient notice period. **5. General Comments:** As Fund Managers do not generally deal with retail customers the Cyber Hygiene notice should not apply to them. As mentioned above, client information is generally held with external service providers (who should be the ones complying with such Cyber Hygiene requirements). If Fund Managers are indeed required to comply, Registered Fund Managers should be exempted given their limited size and scale.
8.	Trendlab Pte. Ltd.	**1. Comments on the applicability of the Notice:** Applicability seems appropriate. **2. Comments on the proposed definitions:** Definitions appear clear. **3. Comments on the proposed cyber security requirements:** Requirements seem to be fairly comprehensive. **4. Comments on the proposed transition period:** We believe that 12 month period is an adequate time to implement and comply with the Notice **5. General Comments:** No comments.
9.	iTGRC Security and Compliance group	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** With respect to the controls area outlined, there may be opportunity to consider paraphrasing “Administrative account” as “Accounts and Password” or “Secured Access”, firewall as “firewall and boundary devices”, security standards as “network and device secured configuration”, Anti-virus as “Malware protection” that expands the definition for wide components coverage – PCs, laptops, mobile devices, servers or virtue machines and etc. There could be an option to include organizational control as such “Training for business and security”, generally refer end user training and awareness. The rationale is to offer friendly terminology to non-technical personnel and enable meaningful impact for organization to thrive in their cyber security readiness and data protection in view of PDPA compliance mandated by PDPC Singapore. **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** Upon multiple discussion and reviews of the notice, we are of the opinion, that the authority may consider including the requirement of a security framework on top of outlining the controls, to enable FSI organizations structure their approach toward achieving the mandates and controls as outlined. On the hindsight of existing TRM which has been emphasizing on Technology Risk Assessment and Treatment option, there remains categories of FSI who desire a holistic know-how to guide them through the journey toward achieving their business goals in adherent to MAS regulatory mandates, in term of rationalizing, planning, design & implementation of the controls. On the same note, Cyber hygiene notice will be of significance value if it suggests organization to build their own cyber hygiene program (CHP) that shall include questionnaires & testing in relevance to the scope of FSI operating environment. CHP will then enable their confidence in supporting any attestation to regulatory review or internal/external audit their controls implementation and effectiveness in responding to breaches, incidents, compliance to regulatory requirements as we as their cyber resilience in totality. Thus, serving a holistic purpose. A cyber hygiene program (CHP) with the inclusion of the above, shall be encouraged independently developed by FSI in accordance to their business context, company value, culture and priority. It should be of a reasonable structure and adaptive in nature, where it not only allows coverage of the 6 controls to start FSI off navigating the path, and also mapping them to a cyber security maturity model that has inputs from local FSI industry which can further resonate and improve the security posture, thus enable them to assess and design more relevant control and activities in relation to their business needs, growth and changes.
10.	Prusik Investment Management Singapore Pte. Ltd	**1. Comments on the applicability of the Notice:** We agree with the proposed coverage of applicable entities. **2. Comments on the proposed definitions:** We are content with the proposed definitions. **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		We have nothing to add to the proposed requirements. **4. Comments on the proposed transition period:** 12 months seems adequate to us. **5. General Comments:** We have no further comments.
11.	Detack GmbH	**1. Comments on the applicability of the Notice:** No Comments. **2. Comments on the proposed definitions:** The IT security landscape as it is affected by technology changes on a constant basis. For this reason, an updated definition of what the current state of the art in IT security is, would be necessary in order for all parties – be it regulatory body, regulated entity, or solution provider – to be able to correctly evaluate and implement the required or recommended controls. We are offering, as a fully functional example of such definition, covering both security and privacy topics, the TeleTrusT yearly publication of the state of the art in IT security definition. The IT Security Association Germany (TeleTrusT) is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations, TeleTrusT embodies the largest competence network for IT security in Germany and Europe. Each year TeleTrusT publishes an updated definition of state of the art in IT security. The publication is being used for defining standards and requirements by government entities and several other regulatory bodies. The publication targets various topics, such as multi factor authentication, password security, and multiple other IT security topics. The 2018 publication can be found, in German language, at: https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ A brief presentation of how the state-of-the-art definition is effectively used is provided in the English language, as attachment A, ETA2018_Definition of State of the Art.pdf. Our proposal is to implement such a definition, regularly updated, for Singapore. This will eliminate confusion in IT

S/N	Respondent	Feedback from respondent
		security related processes, implementation of regulatory requirements, and will provide a common language for all parties involved when addressing and defining threats, appropriate security measures, and disproportionate actions. Such a publication could as well be based on the already existing TeleTrusT paper, adapted to regional requirements. **3. Comments on the proposed cyber security requirements:** In regards to paragraph 9, where it is proposed to require multi-factor authentication for (a) all administrative accounts and for (b) accounts that access confidential data over the Internet, for reasons of process optimization, completeness (full coverage of all systems and environments), as well as better security, we propose the following: Alternative strong authentication: There are systems that do not support multi-factor authentication, or do not support a secure implementation (server-side only) of such technology. There are also accounts that will never support MFA, such as technical accounts, shared support accounts, and process to process communication accounts. In order to provide state of the art, strong authentication for such systems, we propose that the controls in paragraph 9 include, as an alternative for multi-factor authentication, password authentication with quality assurance. Password authentication would be acceptable as an alternative as long as the regulated entity will be able to prove, by quality assurance (password strength measurement) that all passwords used for (a) all administrative accounts and for (b) accounts that access confidential data over the Internet satisfy the security requirements of the data or of the processes they protect. The regulated entity should be able to provide the relevant proof on request. Transition to multi-factor authentication: The transition process to multi-factor authentication often takes a very long time, with challenges at various layers, requiring process changes, vendor changes (products to be modified to support MFA), as well as internal developments. During this process, single-factor authentication will remain in place, potentially for a number of years. During this transition time the regulated entity will not be protected against password-related threats. For this reason, we propose to require or recommend regulated entities to implement password quality assurance (password strength measurement) for the duration of the

S/N	Respondent	Feedback from respondent
		transition process. This will minimize the risk of security compromise due to insecure authentication. A password QA process can be implemented in the largest enterprises in a matter of days, and can be kept active until the multi-factor authentication system is functional for all subject accounts. Completeness of multi-factor authentication: The vast majority of the MFA systems will have a password as one of the factors (the factor the subject knows). If this factor ("the password") is proven weak, then the effectiveness of the multi-facto authentication system will be significantly reduced, in extreme cases down to a single factor. For this reason, we propose to require or recommend regulated entities to implement password quality assurance (password strength measurement) for the password factor in MFA. This will guarantee that the "known factor" in a MFA environment has the required quality. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
12.	Anonymous	Confidential
13.	CME Group Inc.	**1. Comments on the applicability of the Notice:** CME Group Inc. ("CME Group") is the parent of four U.S.-based designated contract markets ("DCMs"): Chicago Mercantile Exchange Inc. ("CME"), Board of Trade of the City of Chicago, Inc. ("CBOT"), New York Mercantile Exchange, Inc. ("NYMEX") and the Commodity Exchange, Inc. ("COMEX") (collectively, the "CME Group Exchanges"). The CME Group Exchanges offer a wide range of products available across all major asset classes, including futures and options based on interest rates, equity indexes, foreign exchange, energy, metals and agricultural commodities. CME also operates a registered swap data repository ("SDR") and CME Clearing, its clearing house division, which is a registered derivatives clearing organization ("DCO") providing clearing and settlement services for exchange-traded and over-the-counter derivatives transactions. The primary regulator for each of these licensed entities is the U.S. Commodities Futures Trading Commission ("CFTC"). At this time, CME, CBOT and NYMEX are each registered with the MAS as a Recognised Market Operator ("RMO"). CME Clearing is registered as a Recognised Clearing House ("RCH") with the MAS. In addition, CME Group has submitted an

S/N	Respondent	Feedback from respondent
		application to the MAS for COMEX to be approved as an RMO and has submitted a second application for CME Trade Repository to be approved as a Licensed Foreign Trade Repository ("LFTR"). In all, CME Group subsidiaries expect to have six separate MAS approvals. CME Group understands the need for the MAS to ensure the cyber resilience of Financial Institutions in Singapore. CME Group has a robust and sound risk management framework to manage the technology and cyber risks. However, CME Group does not agree with the MAS proposal to include entities whose primary regulator is not the MAS in the relevant entities subject to the Notice on Cyber Hygiene. CME Group's view is that entities holding RMO, RCH and LFTR licenses should be primarily regulated by their home regulator which in the case of the CME Group Exchanges, CME SDR and CME Clearing is the CFTC. Our primary concern with the proposed scope of the Notice on Cyber Hygiene is the possibility for significant regulatory overlap and duplicative requirements. We believe the activities of CME Group's licensed entities are already subject to requirements analogous in all material respects to those set forth in the proposed Notice on Cyber Hygiene. Accordingly, we do not think there is any need to extend the scope of this Notice to non-Singapore entities. Moreover, we are concerned that as these rules evolve over time, CME Group could face challenges reconciling the MAS requirements with the requirements of the CFTC. Although we do not see any points of divergence at this time, this could change in the future. If so, entities subject to the Notice on Cyber Hygiene with a primary regulator outside Singapore could be forced to meet multiple contradictory regulatory requirements. This outcome does not seem to fit within the purpose of the RMO, RCH and LFTR regimes established by the MAS. Finally, CME Group is concerned that placing additional regulatory burdens on entities that are not primarily regulated by the MAS would reduce the attractiveness of the RMO, RCH and LFTR regimes and, hence, the attractiveness of Singapore as a place for overseas market infrastructures to carry out activities. **2. Comments on the proposed definitions:** No comments.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
14.	Anonymous	Confidential
15.	Fullerton Fund Management Company Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** 1) Definition of “confidential information” The wordings proposed by MAS under part (b) of the definition of “confidential information” make reference to any information relating or belonging to the relevant entity that is not publicly available. This being broadly worded could have the unintended representation that non-public information, though deemed as immaterial or non-sensitive in nature by the entity, will also fall within scope per the proposed definition. Thus, we suggest that MAS take into consideration of the above and exclude any information relating or belonging to the relevant entity that is not publicly available and not deemed as material or sensitive by the relevant entity from the definition of confidential information. 2) Definition of “security standards” In defining “security standards”, reference is made to a “set of configurations and procedures”. We noted that Annex B of the consultation paper provides some guidance on the measures to address “security standards” requirements. As the measures highlighted are relatively generic, it is not sufficiently clear as to the authorities’ expectations on “configurations and procedures”. It would be useful if some examples can be provided. 3) Definition of “system” Based on the proposed definition of “system”, it is not sufficiently clear if it applies to managed platforms used by the FI. We suggest that more clarity can be included in the definition of “system” in this regard, given that this fundamentally determines the areas that fall within scope of the proposed Notice.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: Multi-factor Authentication Under Point (b), FIs are required to implement the multi-factor authentication for all accounts on any system used by the FI to access confidential information through the internet. While we recognise that this security control should be applied to information accessed through the internet, we would like to clarify if access through the internet should exclude dedicated lease line connectivity and encrypted information. The use of multi-factor authentication has been identified as one of the six cyber hygiene practices that must be implemented. We would like to seek MAS' opinion if other mitigating controls such as periodic monitoring of user activity log can be implemented in lieu of a multi-factor authentication for all accounts on any system used by the FI to access confidential information through the internet. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
16.	Singapore Post Limited	**1. Comments on the applicability of the Notice:** Any licensee under the proposed Payment Services Bill (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) We access to Western Union's systems to provide the remittance services. All system controls are with Western Union, thus does Singpost (just a user of the system) still considered to be under this jurisdiction? If yes, what is the penalty for noncompliance to all the 6 control points? **2. Comments on the proposed definitions:** No further comments. **3. Comments on the proposed cyber security requirements:** - Is SMS OTP acceptable for multi-factor authentication? - Firewall is standard deployment for perimeter defence. Perimeter monitoring like Managed Security Service Providers

S/N	Respondent	Feedback from respondent
		("MSSPs") are equally important to be considered? Will MAS be considering that? - Antivirus technology is no longer effective against the ever evolving malware variants. Industry is going towards Threat Detection & Response ("TDR") and Endpoint Detection & Response ("EDR") solutions. Is MAS considering that? **4. Comments on the proposed transition period:** 12 months grace period from start of notice is reasonable. **5. General Comments:** No comments.
17.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Administrative Accounts – It might be worthwhile to review if the proposed hygiene requirement of securing every administrative account is sufficient enough on account of below – i. The inside attacks are an integral part of the cyber landscape ii. The basic cyber hygiene principles suggest that trust no one in the cyber space iii. Furthermore, more and more of the digital assets continue to move to cloud AND are being managed by third party IT administrators iv. The administrative accounts must have no ability to view/modify the information. This is called as the "separation of duties" in the IT world whereby while Administrators shall be able to do the administrative tasks (say with File Server or Virtual Machine or Database or Storage etc) but they are still not able to see any data in the resource being managed by them. For example, while a Database Administrator shall have the ability to undertake all the administrative tasks expected out of her, she must not be able to make any sense of the data inside the Database being administered as the data is all encrypted. Similarly, the files kept in a file-share server may be all encrypted so that while the system administrator has the ability to administrate the file-share server, he cannot make any sense of the data lying therein.

S/N	Respondent	Feedback from respondent
		v. Essentially, removing the very temptation to look into the data just because an administrator have the ability to do so, shall be the basic hygiene in cyber world. vi. Critical resources shall implement m of n authentication for the administrative functions. Disallowing just one single administrator to be able to change anything shall be the basic hygiene against cyber-attacks. Multi-factor Authentication – it might be worthwhile to review if the proposed hygiene requirement is enough for proving the identities in evolving cyber space. More and more of transactions are application to application OR machine to machine instead of involving the human element. While the human elements are identified reliability through multi-factor authentication (of bio-metrics, PKI, One Time Password etc.), the cyber elements can be reliably be identified by their respective Digital Identities (Private Keys) and Digital Signatures. For example an HTTPS site can only be reliably identified by its SSL keys/certificate or a valid end point in a transaction can only be identified through its corresponding private keys before allowing for the secure session to be established. It shall be considered if hosting these digital identities in secure and tamper-proof hardware shall be the basic cyber hygiene. Furthermore, the digital signatures of the cyber elements shall be periodically confirmed to verify that nothing has changed unknowingly preventing situations whereby the cyber element(s) may have been replaced with unauthorized one(s) causing the entire business and security logic to be bypassed. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
18.	Anonymous	Confidential
19.	Anonymous	Confidential
20.	Anonymous	Confidential
21.	Lloyd’s of London (Asia) Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Happy with most of the definitions, however I think the one relating to “security standards” needs to be a bit more specific.

S/N	Respondent	Feedback from respondent
		It should include actual examples of good practice security standards. The definition on confidential information is wide and recommend for organisations to define their own in accordance to their own policy. **3. Comments on the proposed cyber security requirements:** The requirements provide a set of foundational controls for effectively managing cyber risk and in some respects are very similar to the UK government's Cyber Essential's programme. However, it goes beyond cyber essentials in one important respect, by mandating that entities also have "security standards" but as stated in 2, That requirement will need further elaboration. Request for clarity on the types of systems in scope for security patches and anti-virus, as our understanding of system mentioned in the consultation is wide. Suggest limiting to the Operating System and Cloud-based platform where the risks are higher. **4. Comments on the proposed transition period:** It is a reasonable period of time, however the implementation of multi-factor authentication might need more time. **5. General Comments:** A good set of essential cyber security practices.
22.	Hwee Cher Tan	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** "Security standards" should be more specific – "Operating Systems Security Standard", "Application Configuration Security Standard", "Application Development Security Standard". There should be additional security controls - (a) Network Segmentation: Networks must be organized to provision for data of different levels of sensitivity, different functions, different user groups, different types of access. Access between networks must be restricted by specific IP addresses, service ports and direction of access. Access between networks of high sensitivity and networks of low sensitivity must facilitated by additional authorizations on an intermediate

S/N	Respondent	Feedback from respondent
		network. Inbound access to sensitive networks must be minimized and justified. (b) Monitoring: Alerts must be enabled for real time notification of security events. Audit logs must be enabled for periodic reviews. (c) Incident Management: A proper incident management team and process must be established to minimize the negative impacts. (d) Digital Devices: Digital devices (e.g. personal or corporate smart phones, tablets, laptops) must be screened for hardening setup prior to being granted access to network. Network access by digital devices must be granted based on requirements under "Network Segmentation". (e) Email Filtering: Phishing, spams, malicious attachment, malicious URLs must be blocked. Data loss prevention must be configured. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
23.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** There is no mention of outsourced service providers in the paper. I think the next hot bed of breaches will come from fintech and OSP. As businesses sought to innovate and expand into the digital space quickly, they are slow to catch up on the cyber security aspect and had frequently engage with fintech or offshore OSP who are themselves ill equipped in cyber defences and are poor in Cyber hygiene. As an IT Security practitioner, i have encountered IT companies who simply put their systems on cloud without considerations for IT security and call themselves fintech. They offer a low cost and quick go-to market model which is very attractive to the management/c-suite. It is often an up hill task to convince an offshore vendor to adhere to TRM guidelines when the FI's management are sold on such attractive business propositions. In such scenarios, IT security is often deemed as roadblocks to business and delays to profitable projects by "worrying on things that might not

S/N	Respondent	Feedback from respondent
		happen at all". Such is the attitude even after the massive singhealth. So legalizing this for SG FIs but excluding OSP will not work in my opinion. However, legalizing this for an offshore OSP is also not possible since they are from a different jurisdiction. Seems that it would be what an offshore OSP once told me – "sorry my entity is incorporated in XXX country, we do not need to adhere to MAS guidelines but your CEO needs us". **4. Comments on the proposed transition period:** No comments. **5. General Comments:** While MAS is reacting to the singhealth incident by proposing to legalise cyber hygiene, I think the implications has to be carefully weighed. Firstly, to the less established and FIs without deep pockets, this will directly impact the many men and women (like me) working in cybersecurity. I would think that an FI which is less "security conscious" will not spend more to acquire the tools and manpower to address this but rely on what is current available. This is therefore counter-productive as the cybersecurity workers in such firms will be overworked (if not already so) and the security posture of the industry might not be improved, less those FIs with deep pockets. I feel that a more effective solution should take into consideration factors such as the size/profitability/cyber security budget/resource allocations of FIs when introducing new laws or guidelines. Through such indicators, it will be evident of the management's risk appetite and attitude towards cyber security. And with this, establish nation wide cyber security initiatives/solutions/grants to help those FIs that are more vulnerable. Lastly recognising and improving the morale of cybersecurity workers by empowering them to provide feedback directly to regulators without any consequences. Perhaps setup an MAS affiliated association for all IT security practitioners and separately reinforcing to the C-suite/management board that they are fully accountable in the event of any security incident (if proven due to neglect/mis-management).
24.	Fidelity International	**1. Comments on the applicability of the Notice:** While the draft Notice has set out the types of regulated FIs, which will be subject to the requirements, we request that the MAS give due consideration on the nature, size and complexity

S/N	Respondent	Feedback from respondent
		of the FIs' business operations in Singapore. The sophistication of processes, systems and internal controls for cyber risk management would vary according to these factors. For FIs whose business operations is small, they may be relying on mobile/cloud technology for some level of controls. Hence, the way they comply with these requirements will be different. On the other hand, we recognise that FIs with large business operations or pose systemic impact to Singapore's financial system should have a robust, layered approach to security. The above, however, has not been addressed in the Notice. **2. Comments on the proposed definitions:** These definitions are sufficient and generally consistent in relation to how they are used in the industry. **3. Comments on the proposed cyber security requirements:** 6(a) The wording is quite general and can be interpreted in different ways without necessarily meeting a clear control objective. We suggest that it be re-draft such that there be flexibility accorded to FIs to implement standards and policies that adhere to industry best practices and commensurate with the business information systems. 6(b) We suggest inserting a time factor for the control assurance process. That is, "Subject to sub-paragraph (c), a relevant entity must ensure that its system conform to the set of security standards on a regular basis." 7. Use of a multi-layer firewall approach is not new. Perhaps some guidance around other network layer controls would be useful to the industry. 8. Having one anti-malware measure is not enough to provide sufficient protection. Apart from endpoint protection, e-mail and internet traffic need to be inspected to provide further control to block out malicious attachments or links. Furthermore, controls around removable media should be in place to prevent malware infections or data loss risks. 9(a) Critical systems do require enhanced authentication and monitoring. However, we would like to highlight that not all systems administrator accounts have the capability to enable multi-factor authentication (MFA). Although solutions are available to provide privileged account management, these can

S/N	Respondent	Feedback from respondent
		be costly, complex and/or time consuming for FIs to setup. We also like to point out the following pitfalls around MFA: i) Biometrics tend to fall back to passwords; ii) SMS are increasingly considered insecure; and iii) Email may be an issue depending on the implementation. We are of the view that MAS' concerns over administrative accounts would have been addressed by clause 5 if the FIs regularly apply security patches to its system. **4. Comments on the proposed transition period:** Most of the requirements except for clause 9(a) are fundamental to most FIs and should already be in place. As mentioned above, clause 9(a) poses practical challenges to most FIs. In terms of transition period, 12 months maybe an aggressive timeline for small FIs to conduct gap analysis, secure budget, identify solutions, initiate projects, and implement the requirements. **5. General Comments:** Overall, the requirements are generally basic and most FIs should have a mature posture in place already. In the longer term, providing guidance on industry best practices in a non-prescriptive nature would be more beneficial to FIs as this allows them to implement measures that are appropriate with and commensurate their business model.
25.	Asia Pacific Exchange Pte. Ltd. Asia Pacific Clear Pte. Ltd. (collectively referred to as "APEX")	**1. Comments on the applicability of the Notice:** APEX does not have any comments on the list of entities which have to comply with the requirements in the proposed notice. **2. Comments on the proposed definitions:** "Confidential Information" We think the proposed definition of "Confidential Information" is very broad and may not have included any consideration on the sensitivity of non-publicly available information. Some non-publicly available information may not be sensitive, e.g. • partial or aggregated information of customers which is not sufficiently detailed to identify a particular customer or a particular group of customers; • a relevant entity's internal information (but not confidential), including some internal policies and procedures, organisation chart of a particular department, etc.

S/N	Respondent	Feedback from respondent
		APEX proposes that the definition of "confidential information" could possibly be revised to take into consideration whether the information is sensitive to the customer or relevant entity. One example is the "Private Information" defined by the Office of Qualifications and Examinations Regulation (Ofqual) of UK as follows: == *Private information is information that:* • *relates to an identifiable legal or natural person* • *is not in the public domain or common knowledge* • *would cause them damage, harm or distress if the information were made public* *A 'legal person' is a company or other organisation that has legal rights and duties. A 'natural person' is a member of the public. Where we use the term 'individual' in our publications it means both legal and natural persons, both living and dead. Information that is lawfully in the public domain and readily available to the public does not automatically become confidential when it is used to produce a statistic.* *https://www.gov.uk/government/publications/ofquals-statistics-policies-and-procedures/statement-on-confidentiality* == In respect of limb (a) of the definition, where specific classes of financial institutions are subject to obligations under the respective legislations (e.g. the Securities and Futures Act) to maintain confidentiality of user information, MAS may wish to consider aligning limb (a) of the definition of "Confidential Information" in the proposed Notice with such established definition of user information. This would avoid implementation issues across different definitions and obligations. "Multi-factor Authentication" The proposed definition does not appear to cover the use of SMS. For the avoidance of doubt, APEX would like to clarify with the MAS whether One-Time Password (OTP) via SMS would be allowed to be used as one of the factors in a multi-factor authentication setup. **3. Comments on the proposed cyber security requirements:** APEX does not have further comments on the proposed cyber security requirements

S/N	Respondent	Feedback from respondent
		4. Comments on the proposed transition period: APEX would like to propose an 18-month transition period for the implementation of the MFA requirement as we foresee resourcing issues to meet the requirement for administrative accounts. Other than that, we are supportive of the 12-month transition period for the rest of the requirements in the proposed Notice. **5. General Comments:** APEX is generally supportive of the proposed notice on cyber hygiene, and agrees that the introduction of the notice is particular pertinent given the increase in cyber security breach incidents that have been reported and the increase in the use of technology in the financial industry.
26.	Anonymous	Confidential
27.	Transamerica Life (Bermuda) Ltd	**1. Comments on the applicability of the Notice:** No comments **2. Comments on the proposed definitions:** Does ‘system failure’ refer to availability or confidentiality & integrity failure? **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
28.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** (i) Definition on “confidential information” (b) any information relating or belonging to the relevant entity that is not publicly available; The qualifier “any” in point (b) is too wide as there is much non-confidential information belonging to the entity that is not available publicly. Perhaps, could consider using either information internally classified as confidential or higher that is not publicly available or exclude information internally classified as below confidential.

S/N	Respondent	Feedback from respondent
		By using the original definition, as entities usually do not tag information as publicly available or not, hence all information will need to be classified as confidential incurring a burden to encrypt them throughout their life cycle. For clarity, we propose to use similar definition provided by PDPA 2012 for "personal data" but restricted to "personal data" which are not publicly available. (ii) Part (b) definition of "critical system" i.e. "provides essential services to customers" Reference is made to MAS Guidelines on Internet Banking and Technology Risk Management. For clarity, part (b) should be referring to online financial services offered via internet. We propose to revise part (b) to "provides via internet essential online financial services and products to customers". **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** 12 month period is a reasonable transition. **5. General Comments:** No other comments.
29.	HSH Nordbank Singapore Branch	**1. Comments on the applicability of the Notice:** No further comments as the coverage is sufficient. **2. Comments on the proposed definitions:** No further comments as the definitions are clear. **3. Comments on the proposed cyber security requirements:** HSH would recommend to add an additional measure "External Penetration Test" as this is a good practice for FI to further enhance it's Cyber defence. **4. Comments on the proposed transition period:** The time line is reasonable. **5. General Comments:** No comments.
30.	ABN AMRO Bank N.V., Singapore Branch	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Additions:

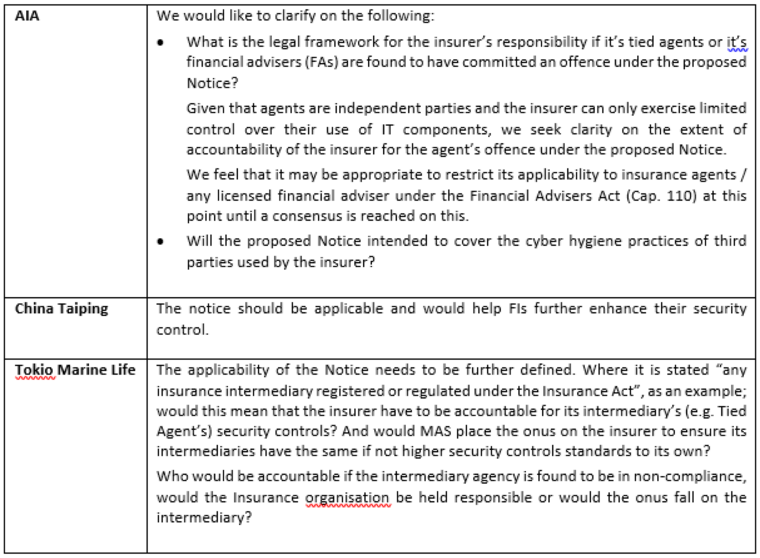
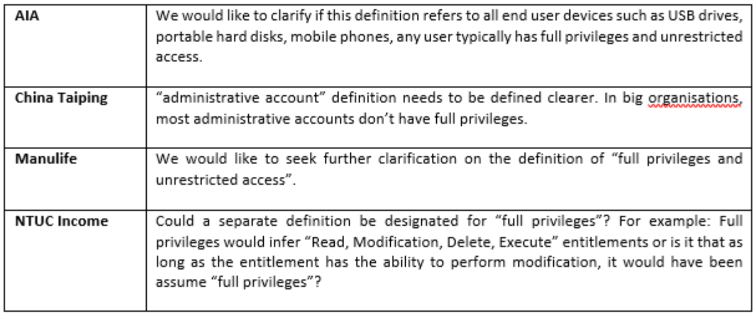
S/N	Respondent	Feedback from respondent
		- "administrative account": add an "or" to: "…privileges and/or unrestricted access…" - In line with Annex B, Para 9, "confidential information" should receive sub point (c) any information relating to, or any particulars of, any employee of the relevant entity, that is not publicly available; - "critical system": should receive a sub point (c) contains information relating to, or any particulars of, any customer information that is not publicly available; And an "or" should be added to the end of sub point (b). - "multi factor authentication": should receive a sub point (d) something that restricts based upon device identity; - "system" should be amended by the sentence: or any IoT (Internet of Things) device that provides a potential entry vector into the network of the relevant entity;. Could MAS clarify if a smartcard (containing a personal certificate) with an associated PIN is considered as "multi-factor authentication"? **3. Comments on the proposed cyber security requirements:** Hygiene should not be a one-time implementation, but a continuous process. Therefore the following should be added/amended to/in the Chapter: Cyber Hygiene Practises: ADD: 4.1 The relevant entity must implement a control process that ensures a 6-months review cycle for every administrative or high privileged account. ADD: 4.2 Any use of administrative or high privileged accounts needs to be electronically documented. The integrity of these usage logs needs to be ensured. ADD: 5 (a-1) A relevant entity must implement a documented process that clarifies the entity's strategy to identify Security Patches. A register of identified Security Patches shall be kept that includes the reasoning for any identified, but non-deployed Security Patch and the respective risk mitigation strategy. AMEND: 6 (a) "… systems, as well as administrative accounts and preventive measures. This document also has to contain an annual review cycle for the security standards. The security standards must include the procedures for penetration testing of new applications, as well as source code reviews."

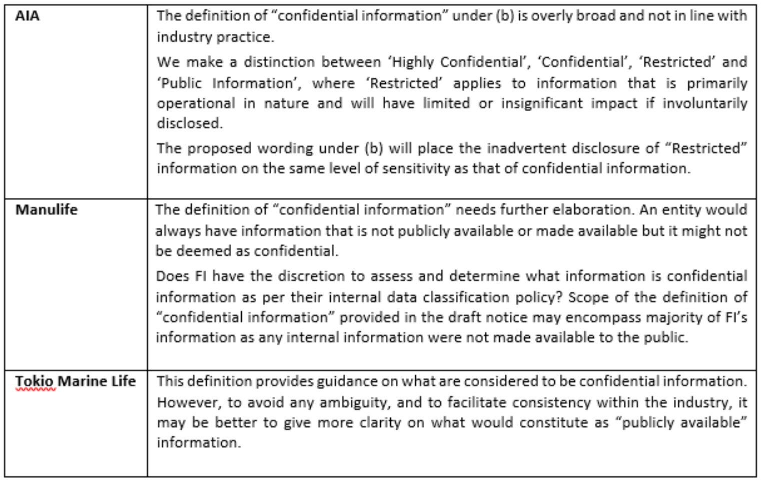
S/N	Respondent	Feedback from respondent
		ADD: 7 In case of multi-national entities or similarly structured entities, where any given part resides in a country with lesser security standards than Singapore, one or more firewalls have to be implemented between the entities to ensure the security of the Singaporean relevant entity. AMEND: 9 (b) "…confidential or personally identifiable information that is not publicly available through …" A new item should be added on access to systems via removable media, for example, but not limited to, devices attached to USB ports. This is also in line with the requirements stipulated in the MAS Circular MAS/TRS/2017/51 and it's amendments. Potentially: ADD: The relevant entity must ensure that unauthorized access to systems cannot be achieved via open port attack vectors like e.g., but not limited to, USB. The handling of these potential attack vectors must be documented in the security standards that the relevant entity maintains, and a log of these accesses must be kept. Section 7 Firewall a) Could MAS clarify if internal network segregation protected by firewalls must be implemented. Internal segregation could be desirable to segregate networks based on their purpose (e.g. development, testing, and production) or security levels (e.g. SWIFT systems, core banking systems), in line with MAS TRM section 9.3.4 requirements? b) Could MAS clarify why only firewalls are listed while other MAS publications such as Circular No. SRD TR 01/2015 requires the deployment of Intrusion Detection / Prevention Systems? Does that mean that Circular No. SRD TR 01/2015 is now obsolete? Section 8 Anti-virus Could MAS clarify why only traditional anti-viruses are mentioned while other MAS publications such as Circular No. SRD TR 01/2009 on endpoint security and data protection require implementation of Data Loss Prevention (DLP) solutions, and Advanced Persistent Threat (APT). Does this notice make those previous publications obsolete? Section 9 Multi-factor authentication This section seems to be applicable to critical systems only while MAS TRMG section 11.2.3 does not make that distinction and requires implementation of two-factor authentication for

S/N	Respondent	Feedback from respondent
		privileged access regardless of the system criticality. Could MAS clarify which requirement is applicable going forward? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** In light of "MAS/TRS/2017/51 MAS Advisory on Security of Wholesale Payment Systems and Terminals", which will just be defined as system under this notice, the guidance to comply with cyber hygiene requirements (Annex B) should be revisited. Annex B in general softens the Cyber Hygiene by making use of words like can instead of must. Also by pointing out that depending on scale, complexity and nature of business of different entities, without giving clear guidance on these Key Indicators, any relevant entity can decide for themselves what to implement. E.g. Para 7 says "… must implement one or more firewalls…" where Annex B then gives an arbitrary choice based upon the non-defined Indicators to Para 7 "Implement one or more firewalls…".
31.	Anonymous	Confidential
32.	Arab Banking Corporation (B.S.C.), Singapore Branch	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** (A) In paragraph 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." *Bank ABC's comment:* The statement "within a timeframe that is commensurate with the risks" should be more specific for example, for instance SWIFT security requirements, suggesting to indicate: • Critical (9.0+ score): applied within 1 month of release • High (7.0 - 8.9 score): applied within 2 months of release • Low / Medium (< 7.0 score): user defined Kindly Note: the score is based on the CVSS global market standard.

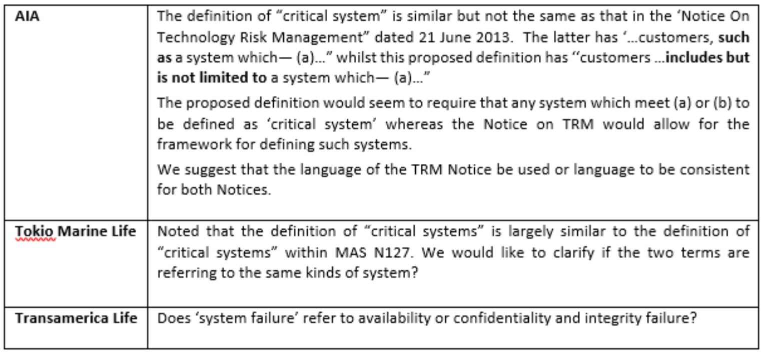
S/N	Respondent	Feedback from respondent
		(B) In paragraph 7 Firewall: "A relevant entity must implement one or more firewalls at its network perimeter to restrict all unauthorised network traffic." *Bank ABC's comment*: An organisation has one or more firewalls on the perimeter for high availability purposes however it may be more helpful to indicate that an organisation should follow a multi-tier firewall approach where there is a firewall to protect the perimeter and also one or more inside firewalls to protect internal network segments. (C) In paragraph 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." *Bank ABC's comment*: In relation to paragraph 9(a), the statement should be more specific and make reference to for example, all IT systems and security administration accounts on its core infrastructure systems (e.g., firewalls), operating systems and database engines. In relation to paragraph 9(b), it should not be limited to accessing the system through the internet. Rather, it is about users who access the system also have access to the internet and/or to receiving external emails. In addition, there should be more guidance on what MAS considers minimum confidential information e.g., customers' personal details, payments details, financial records. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
33.	Association of Independent Asset Managers Singapore (AIAM)	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** The definition of "system" seems to imply all IT components and is very broad. Can MAS define and give specific examples for these systems where the administrative accounts need to be secured? **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		Administrative Accounts: Can MAS define and give specific examples for these systems where the administrative accounts need to be secured? Applying Security Patches Within Timeframe Commensurate With Vulnerability Risk: Where a security patch has reached its end-of-support and is no longer being updated by its vendors, what is a reasonable timeframe for transition to a new solution and can MAS guide on how this varies if vulnerabilities risk is low or high? Written Set of Security Standards: While it is technically possible for each firm to come up with their own security standards, it may differ widely across the industry. Can MAS provide guidelines on the security standards requirements that they need from external asset managers? Also, what are suggested security standards for cloud services? Multi-factor Authentication - Systems providers are generally able to provide two factor authentication but this is at an additional fee and implementation would inevitably increase the cost of business. Also can MAS provide more examples and case studies where multi-factor authentication is required to expand on situations 9(a) and (b)? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.

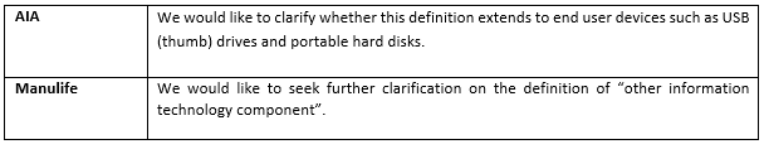
<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td>34.</td><td>Life Insurance Association, Singapore</td><td>
<b>1. Comments on the applicability of the Notice:</b>

<table>
<tr><td><b>AIA</b></td><td>We would like to clarify on the following:
• What is the legal framework for the insurer's responsibility if it's tied agents or it's financial advisers (FAs) are found to have committed an offence under the proposed Notice?
Given that agents are independent parties and the insurer can only exercise limited control over their use of IT components, we seek clarity on the extent of accountability of the insurer for the agent's offence under the proposed Notice.
We feel that it may be appropriate to restrict its applicability to insurance agents / any licensed financial adviser under the Financial Advisers Act (Cap. 110) at this point until a consensus is reached on this.
• Will the proposed Notice intended to cover the cyber hygiene practices of third parties used by the insurer?</td></tr>
<tr><td><b>China Taiping</b></td><td>The notice should be applicable and would help FIs further enhance their security control.</td></tr>
<tr><td><b>Tokio Marine Life</b></td><td>The applicability of the Notice needs to be further defined. Where it is stated "any insurance intermediary registered or regulated under the Insurance Act", as an example; would this mean that the insurer have to be accountable for its intermediary's (e.g. Tied Agent's) security controls? And would MAS place the onus on the insurer to ensure its intermediaries have the same if not higher security controls standards to its own?
Who would be accountable if the intermediary agency is found to be in non-compliance, would the Insurance organisation be held responsible or would the onus fall on the intermediary?</td></tr>
</table>
<b>2. Comments on the proposed definitions:</b>
<i>"administrative account", in relation to a system, means any user account that has full privileges and unrestricted access to the system;</i>

<table>
<tr><td><b>AIA</b></td><td>We would like to clarify if this definition refers to all end user devices such as USB drives, portable hard disks, mobile phones, any user typically has full privileges and unrestricted access.</td></tr>
<tr><td><b>China Taiping</b></td><td>"administrative account" definition needs to be defined clearer. In big organisations, most administrative accounts don't have full privileges.</td></tr>
<tr><td><b>Manulife</b></td><td>We would like to seek further clarification on the definition of "full privileges and unrestricted access".</td></tr>
<tr><td><b>NTUC Income</b></td><td>Could a separate definition be designated for "full privileges"? For example: Full privileges would infer "Read, Modification, Delete, Execute" entitlements or is it that as long as the entitlement has the ability to perform modification, it would have been assume "full privileges"?</td></tr>
</table>
<i>"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;</i>
</td></tr>
</table>

<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td>

<table>
<tr><td><b>AIA</b></td><td>The definition of “confidential information” under (b) is overly broad and not in line with industry practice.
We make a distinction between ‘Highly Confidential’, ‘Confidential’, ‘Restricted’ and ‘Public Information’, where ‘Restricted’ applies to information that is primarily operational in nature and will have limited or insignificant impact if involuntarily disclosed.
The proposed wording under (b) will place the inadvertent disclosure of “Restricted” information on the same level of sensitivity as that of confidential information.</td></tr>
<tr><td><b>Manulife</b></td><td>The definition of “confidential information” needs further elaboration. An entity would always have information that is not publicly available or made available but it might not be deemed as confidential.
Does FI have the discretion to assess and determine what information is confidential information as per their internal data classification policy? Scope of the definition of “confidential information” provided in the draft notice may encompass majority of FI’s information as any internal information were not made available to the public.</td></tr>
<tr><td><b>Tokio Marine Life</b></td><td>This definition provides guidance on what are considered to be confidential information. However, to avoid any ambiguity, and to facilitate consistency within the industry, it may be better to give more clarity on what would constitute as “publicly available” information.</td></tr>
</table>

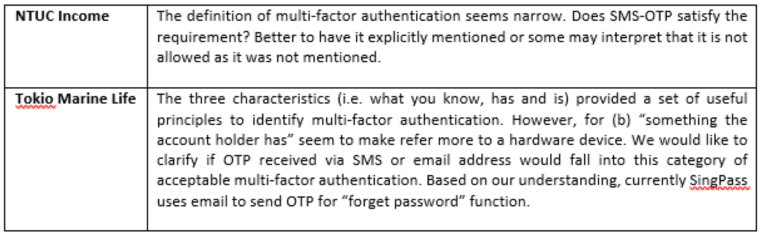
<i>“critical system” in relation to a relevant entity, means a system, the failure of which will cause significant disruption to the operations of the relevant entity or materially impact the relevant entity’s service to its customers. A critical system includes but is not limited to a system which —
(a) processes transactions that are time critical; or
(b) provides essential services to customers;</i>

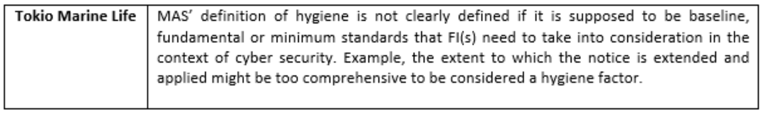

<table>
<tr><td><b>AIA</b></td><td>The definition of “critical system” is similar but not the same as that in the ‘Notice On Technology Risk Management” dated 21 June 2013. The latter has ‘…customers, <b>such as</b> a system which— (a)…” whilst this proposed definition has ‘‘customers …<b>includes but is not limited to</b> a system which— (a)…”
The proposed definition would seem to require that any system which meet (a) or (b) to be defined as ‘critical system’ whereas the Notice on TRM would allow for the framework for defining such systems.
We suggest that the language of the TRM Notice be used or language to be consistent for both Notices.</td></tr>
<tr><td><b>Tokio Marine Life</b></td><td>Noted that the definition of “critical systems” is largely similar to the definition of “critical systems” within MAS N127. We would like to clarify if the two terms are referring to the same kinds of system?</td></tr>
<tr><td><b>Transamerica Life</b></td><td>Does ‘system failure’ refer to availability or confidentiality and integrity failure?</td></tr>
</table>

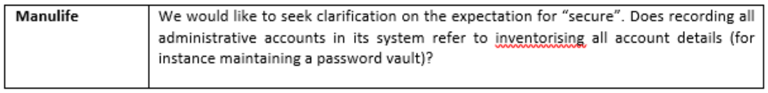
<i>“system”, in relation to a relevant entity, means any hardware, software, network, or other information technology (“IT”) component used by the relevant entity;</i>

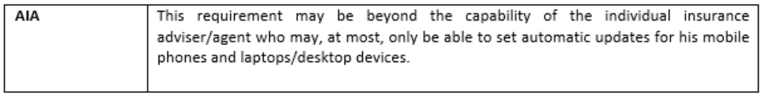

<table>
<tr><td><b>AIA</b></td><td>We would like to clarify whether this definition extends to end user devices such as USB (thumb) drives and portable hard disks.</td></tr>
<tr><td><b>Manulife</b></td><td>We would like to seek further clarification on the definition of “other information technology component”.</td></tr>
</table>

<i>“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;</i>
</td></tr>
</table>

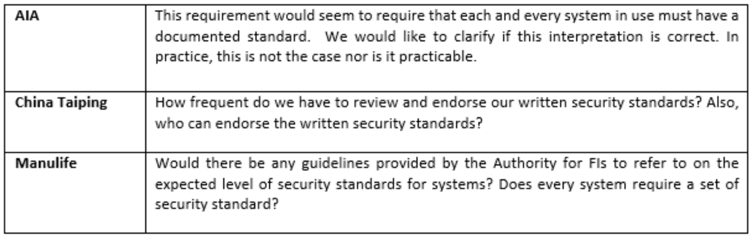
<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td>
<i>(b) something that the account holder has such as a cryptographic identification device or token;</i>
<i>(c) something that the account holder is such as an account holder’s biometrics or his behaviour;</i>

<table>
<tr><td><b>NTUC Income</b></td><td>The definition of multi-factor authentication seems narrow. Does SMS-OTP satisfy the requirement? Better to have it explicitly mentioned or some may interpret that it is not allowed as it was not mentioned.</td></tr>
<tr><td><b>Tokio Marine Life</b></td><td>The three characteristics (i.e. what you know, has and is) provided a set of useful principles to identify multi-factor authentication. However, for (b) “something the account holder has” seem to make refer more to a hardware device. We would like to clarify if OTP received via SMS or email address would fall into this category of acceptable multi-factor authentication. Based on our understanding, currently SingPass uses email to send OTP for “forget password” function.</td></tr>
</table>

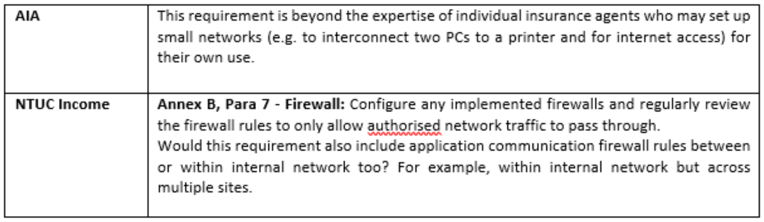
<i>Other comments</i>

<table>
<tr><td><b>Tokio Marine Life</b></td><td>MAS’ definition of hygiene is not clearly defined if it is supposed to be baseline, fundamental or minimum standards that FI(s) need to take into consideration in the context of cyber security. Example, the extent to which the notice is extended and applied might be too comprehensive to be considered a hygiene factor.</td></tr>
</table>

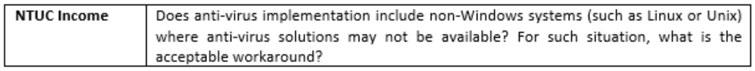
<b>3. Comments on the proposed cyber security requirements:</b>
<i>Administrative Accounts: A relevant entity must secure every administrative account on its system to prevent any unauthorised access to or use of, such account.</i>

<table>
<tr><td><b>Manulife</b></td><td>We would like to seek clarification on the expectation for “secure”. Does recording all administrative accounts in its system refer to inventorising all account details (for instance maintaining a password vault)?</td></tr>
</table>

<i>Security Patches:</i>
<i>(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.</i>
<i>(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.</i>

<table>
<tr><td><b>AIA</b></td><td>This requirement may be beyond the capability of the individual insurance adviser/agent who may, at most, only be able to set automatic updates for his mobile phones and laptops/desktop devices.</td></tr>
</table>

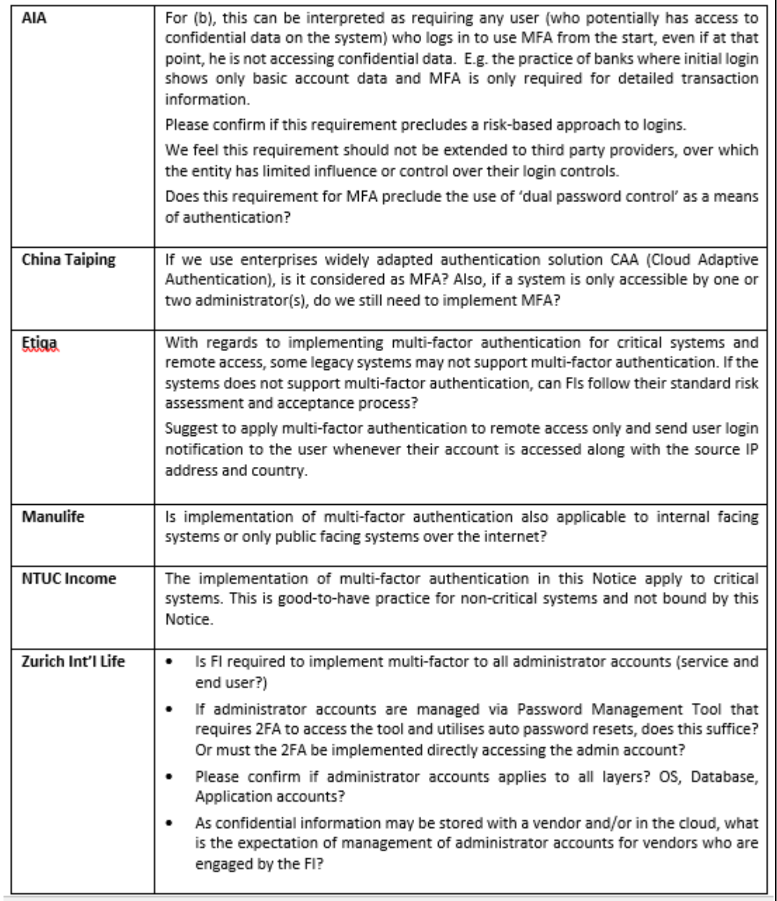
<i>Security Standards:</i>
<i>(a) A relevant entity must have a written set of security standards for its system.</i>
<i>(b) Subject to sub-paragraph (c), a relevant entity must ensure that its system conform to the set of security standards.</i>
<i>(c) Where the system is unable to conform to the set of security standards, the relevant entity must institute controls to reduce any risk posed by such non-conformity.</i>
</td></tr>
</table>

<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td>

<table>
<tr><td><b>AIA</b></td><td>This requirement would seem to require that each and every system in use must have a documented standard. We would like to clarify if this interpretation is correct. In practice, this is not the case nor is it practicable.</td></tr>
<tr><td><b>China Taiping</b></td><td>How frequent do we have to review and endorse our written security standards? Also, who can endorse the written security standards?</td></tr>
<tr><td><b>Manulife</b></td><td>Would there be any guidelines provided by the Authority for FIs to refer to on the expected level of security standards for systems? Does every system require a set of security standard?</td></tr>
</table>

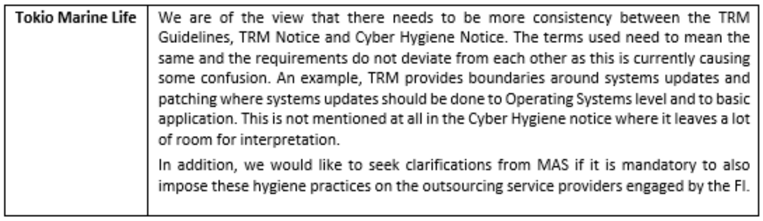
<i>Firewall: A relevant entity must implement one or more firewalls at its network perimeter to restrict all unauthorised network traffic.</i>

<table>
<tr><td><b>AIA</b></td><td>This requirement is beyond the expertise of individual insurance agents who may set up small networks (e.g. to interconnect two PCs to a printer and for internet access) for their own use.</td></tr>
<tr><td><b>NTUC Income</b></td><td><b>Annex B, Para 7 - Firewall:</b> Configure any implemented firewalls and regularly review the firewall rules to only allow authorised network traffic to pass through.
Would this requirement also include application communication firewall rules between or within internal network too? For example, within internal network but across multiple sites.</td></tr>
</table>

<i>Anti-virus: A relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system</i>

<table>
<tr><td><b>NTUC Income</b></td><td>Does anti-virus implementation include non-Windows systems (such as Linux or Unix) where anti-virus solutions may not be available? For such situation, what is the acceptable workaround?</td></tr>
</table>

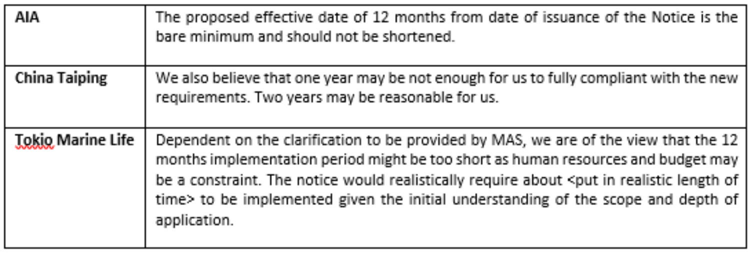
<i>Multi-factor Authentication: A relevant entity must implement multi-factor authentication for the following:
(a) all administrative accounts on its critical system; and
(b) all accounts on any system used by the relevant entity to access confidential information through the internet.</i>
</td></tr>
</table>

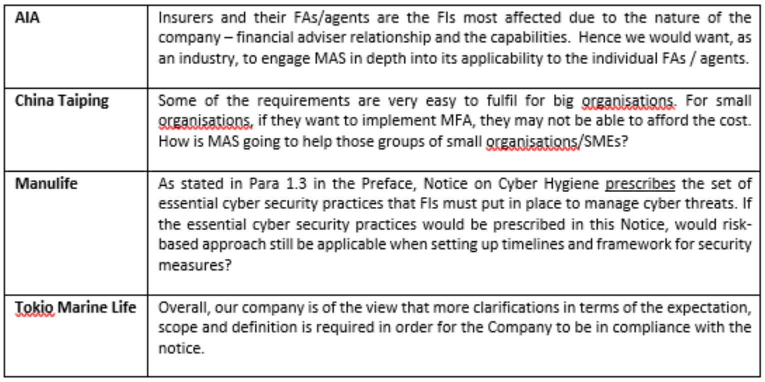
<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td>

<table>
<tr><td>AIA</td><td>For (b), this can be interpreted as requiring any user (who potentially has access to confidential data on the system) who logs in to use MFA from the start, even if at that point, he is not accessing confidential data. E.g. the practice of banks where initial login shows only basic account data and MFA is only required for detailed transaction information.
Please confirm if this requirement precludes a risk-based approach to logins.
We feel this requirement should not be extended to third party providers, over which the entity has limited influence or control over their login controls.
Does this requirement for MFA preclude the use of 'dual password control' as a means of authentication?</td></tr>
<tr><td>China Taiping</td><td>If we use enterprises widely adapted authentication solution CAA (Cloud Adaptive Authentication), is it considered as MFA? Also, if a system is only accessible by one or two administrator(s), do we still need to implement MFA?</td></tr>
<tr><td>Etiqa</td><td>With regards to implementing multi-factor authentication for critical systems and remote access, some legacy systems may not support multi-factor authentication. If the systems does not support multi-factor authentication, can FIs follow their standard risk assessment and acceptance process?
Suggest to apply multi-factor authentication to remote access only and send user login notification to the user whenever their account is accessed along with the source IP address and country.</td></tr>
<tr><td>Manulife</td><td>Is implementation of multi-factor authentication also applicable to internal facing systems or only public facing systems over the internet?</td></tr>
<tr><td>NTUC Income</td><td>The implementation of multi-factor authentication in this Notice apply to critical systems. This is good-to-have practice for non-critical systems and not bound by this Notice.</td></tr>
<tr><td>Zurich Int'l Life</td><td>• Is FI required to implement multi-factor to all administrator accounts (service and end user?)
• If administrator accounts are managed via Password Management Tool that requires 2FA to access the tool and utilises auto password resets, does this suffice? Or must the 2FA be implemented directly accessing the admin account?
• Please confirm if administrator accounts applies to all layers? OS, Database, Application accounts?
• As confidential information may be stored with a vendor and/or in the cloud, what is the expectation of management of administrator accounts for vendors who are engaged by the FI?</td></tr>
</table>

Other comments


<table>
<tr><td>Tokio Marine Life</td><td>We are of the view that there needs to be more consistency between the TRM Guidelines, TRM Notice and Cyber Hygiene Notice. The terms used need to mean the same and the requirements do not deviate from each other as this is currently causing some confusion. An example, TRM provides boundaries around systems updates and patching where systems updates should be done to Operating Systems level and to basic application. This is not mentioned at all in the Cyber Hygiene notice where it leaves a lot of room for interpretation.
In addition, we would like to seek clarifications from MAS if it is mandatory to also impose these hygiene practices on the outsourcing service providers engaged by the FI.</td></tr>
</table>

4. Comments on the proposed transition period:


<table>
<tr><td>AIA</td><td>The proposed effective date of 12 months from date of issuance of the Notice is the bare minimum and should not be shortened.</td></tr>
<tr><td>China Taiping</td><td>We also believe that one year may be not enough for us to fully compliant with the new requirements. Two years may be reasonable for us.</td></tr>
<tr><td>Tokio Marine Life</td><td>Dependent on the clarification to be provided by MAS, we are of the view that the 12 months implementation period might be too short as human resources and budget may be a constraint. The notice would realistically require about <put in realistic length of time> to be implemented given the initial understanding of the scope and depth of application.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td><b>5. General Comments:</b>

<table>
<tr><td>AIA</td><td>Insurers and their FAs/agents are the FIs most affected due to the nature of the company – financial adviser relationship and the capabilities. Hence we would want, as an industry, to engage MAS in depth into its applicability to the individual FAs / agents.</td></tr>
<tr><td>China Taiping</td><td>Some of the requirements are very easy to fulfil for big organisations. For small organisations, if they want to implement MFA, they may not be able to afford the cost. How is MAS going to help those groups of small organisations/SMEs?</td></tr>
<tr><td>Manulife</td><td>As stated in Para 1.3 in the Preface, Notice on Cyber Hygiene prescribes the set of essential cyber security practices that FIs must put in place to manage cyber threats. If the essential cyber security practices would be prescribed in this Notice, would risk-based approach still be applicable when setting up timelines and framework for security measures?</td></tr>
<tr><td>Tokio Marine Life</td><td>Overall, our company is of the view that more clarifications in terms of the expectation, scope and definition is required in order for the Company to be in compliance with the notice.</td></tr>
</table>

<u>LLA's Feedback:</u>
Does the Notice apply to Exempt Financial Adviser Representatives (tied agents)? If yes, to what extent, if any, would their Exempt Financial Advisers (insurers) be held responsible for their tied agents' compliance or non-compliance with the requirements under the Notice? If yes, the industry would be concerned because tied agents are not in a position to comply with some requirements due to technical factors, e.g. individuals cannot generate 2FA verification. In this case, we would be grateful to be given an opportunity to discuss this further with MAS.</td></tr>
<tr><td>35.</td><td>Maybank Singapore</td><td>Confidential</td></tr>
<tr><td>36.</td><td>Anonymous</td><td><b>1. Comments on the applicability of the Notice:</b>
No comments.

<b>2. Comments on the proposed definitions:</b>
No comments.

<b>3. Comments on the proposed cyber security requirements:</b>
Implementing MFA is complex and not straight forward for certain operating systems like Unix/Solaris, hence there must be some flexibility to accept other alternatives like IAM (privilege account access).

<b>4. Comments on the proposed transition period:</b>
The effective date of 12 months from date of issuance of the Notice is not adequate to complete the deployment of security control effectively under the current internal and external circumstances in particular manpower and vendor competencies. Generally, product sourcing, evaluation, selection, negotiation, budgeting process will take around 12</td></tr>
</table>

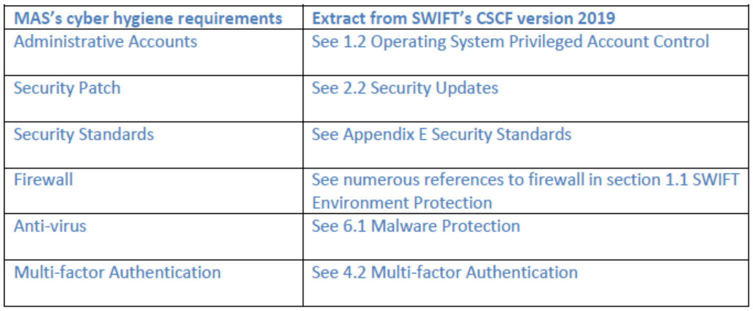
S/N	Respondent	Feedback from respondent
		months. In addition, deployment (SIT, UAT) process will take 3 months at least depending on resources. **5. General Comments:** No comments.
37.	Rabobank Singapore Branch	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** • In relation to the definition of "administrative account" could we include "service or non-interactive accounts" (not just user accounts) that may have full privileges or unrestricted access to the system as an administrator account. • In relation to the definition of "confidential information", we are of the view that the definition should be further restricted to cover the more riskier and sensitive information that is not publicly available and not just any type of information that is not publicly available because a lot of information that the bank holds is not publicly available. However, these are not necessarily sensitive and may not necessarily need to be protected under this new Notice. • A "system" is defined as "any hardware, software, network or any IT other components". We ask that this be reviewed and narrowed down further because at the moment it covers too wide a spectrum which will impact the implementation of this Notice as banks might have difficulty complying with Paragraphs 4, 5, 6, 8 and 9 of the draft Notice across an all-encompassing array of items. A system should be pre-defined to conduct certain types of activities. **3. Comments on the proposed cyber security requirements:** • For Paragraph 5(b), we suggest that this also covers the scenario where a patch is available, but cannot be applied for various valid reasons. Hence, the revision should be: "Where no security patch is available to address the identified vulnerability or the available patch cannot be applied, the relevant entity must institute controls to reduce any risk posted by such vulnerability to its system". • For paragraph 6 Security Standards, we would like MAS to consider allowing banks to comply with security standards set out on a risk based approach based on an IT risk framework approved by banks' boards of directors or senior management. • For paragraph 9 Multi-Factor Authentication, we would like MAS to: ✓ provide clarification to the terms "system" and "confidential information" in paragraph 9(b) as the

S/N	Respondent	Feedback from respondent
		proposed definitions used in this context seems too broad. For example, if the bank allows confidential information to be accessed by the staff through the internet (for example, an HR system hosted in the cloud), does this mean that multifactor authentication must be used on all of the hardware components that work together to provide access to the cloud based server, including the routers, switches, web proxy servers, firewalls etc or is multifactor authentication required only within the cloud based application itself and not the hardware components that are used to provide access to it? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
38.	Anonymous	Confidential
39.	SWIFT	**1. Comments on the applicability of the Notice:** As recommended below (5. General Comments), we believe it makes sense to consider different categories of classification in the Notice. While all entities are likely to benefit from sound cyber hygiene practices, the effort required should be in line with the complexity of each entity's systems and processes. **2. Comments on the proposed definitions:** "administrative accounts" – SWIFT suggests to first define administrator. We suggest that an administrator may refer to: • Application Administrators – responsible for configuring, maintaining, and conducting privileged activities through an application interface • System Administrators – responsible for configuring, maintaining, and conducting other privileged activities via operating systems or other direct (non front-end) access "multi-factor authentication" – SWIFT suggests the use of the following definition: Multi-factor authentication is a method of user authentication where at least two different components are required to authenticate a user. The following authentication factors can be selected:

S/N	Respondent	Feedback from respondent

- Knowledge factor (something the user knows), for example, a PIN or a password
- Possession factor (something the user has), for example, an HSM token, a Digipass, mobile phone, or an RSA One Time Password device
- Human factor (something the user is), for example, finger print or any other biometric

3. Comments on the proposed cyber security requirements:
SWIFT recommends evolving the cyber hygiene requirements to a more principle-based set of guidelines. Find below a table comparing MAS's six requirements with SWIFT Customer Security Controls Framework's controls and measures.



MAS's cyber hygiene requirements	Extract from SWIFT's CSCF version 2019
Administrative Accounts	See 1.2 Operating System Privileged Account Control
Security Patch	See 2.2 Security Updates
Security Standards	See Appendix E Security Standards
Firewall	See numerous references to firewall in section 1.1 SWIFT Environment Protection
Anti-virus	See 6.1 Malware Protection
Multi-factor Authentication	See 4.2 Multi-factor Authentication

4. Comments on the proposed transition period:
Depending on the complexity of the systems and processes of impacted institutions it is probably more adequate to allow more time (up to 18 months) for more complex environments ("complex" profile) to implement the requirements.

5. General Comments:
SWIFT supports MAS's initiative to issue a Notice on Cyber Hygiene. Essential cybersecurity practices are minimum requirements to put in place for any institution to manage cyber threats and enable the security of the broader financial ecosystem.

<u>A broad, principle based framework is required</u>
SWIFT respectfully suggests that MAS might want to a take broader approach that goes beyond the six proposed controls and covers technology, processes and people. The MAS might also consider defining a principle, objective and risk-based framework, such as those promulgated by other regulators around the world. Any such framework would need to recognise the varying architectures and technology implementations of supervised institutions, and should ideally map to other

S/N	Respondent	Feedback from respondent
		frameworks in order to avoid overlap and duplication for your supervised institutions. Examples include: • CPMI-IOSCO's Guidance on Cyber Resilience (June 2016)1: This document provides guidance to Financial Market Infrastructures and provides the various areas which need to be taken into account when an institution sets up its cyber defence. The guidance includes sections on: (1) cyber governance, (2) identification of critical operations and assets, (3) appropriate protection, (4) detection mechanisms, (5) response and recovery, (6) testing, (7) situational awareness and (8) learning and evolving. • New York Department of Financial Services' (NYDFS) cybersecurity requirements for financial services companies (January 2017)2: These New York state rules and regulations require financial institutions to adopt a cybersecurity programme and imposes minimum standards. The requirements include following sections (non-exhaustive): (1) maintain a cybersecurity programme, (2) set up a cybersecurity policy, (3) appointment of Chief Information Security Officer, (4) penetration testing and vulnerability assessments, (5) ensuring audit trails, (6) controlling access privileges, (7) ensuring application security, (8) risk assessment, (9) cybersecurity personnel and intelligence, (10) third party service provider security policy, (11) training and monitoring and (12) incident response plan. • European Banking Authority's (EBA) guidelines on the security measures for operational and security risks of payment services (December 2017)3: EBA created these guidelines as part of the Payment Services Directive review which demands that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage operational and security risks relating to the payment services they provide. These guidelines includes sections on: (1) governance, (2) risk management, (3) protection, (4) detection, (5) business continuity, (6) testing, (7) situational awareness and continuous learning. SWIFT's own Customer Security Control Framework (CSCF)4 could provide a useful basis for the MAS if it were to consider such an approach. Part of SWIFT's Customer Security Programme (CSP), the CSCF describes a set of mandatory and advisory security controls for SWIFT users. All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and

S/N	Respondent	Feedback from respondent
		Limit Access', and 'Detect and Respond'. These objectives refer to a comprehensive set of technology, process and people security controls, and establish a minimum security baseline for the local operating environments of all SWIFT users. SWIFT has chosen to prioritise specific mandatory controls to set a realistic goal for short-term, tangible security gain and risk reduction. Advisory controls are based on good practice that SWIFT recommends users implement. Over time, mandatory controls may change due to evolving threats, and some advisory controls may become mandatory. Each control is defined with a control objective, risk drivers, list of in-scope components and SWIFT guidelines for implementation. SWIFT users may choose either to implement SWIFT guidelines or choose alternative implementations as long as they comply with the control objective, mitigate risk and cover all in-scope components. This affords users flexibility, while also meeting the objective of the control and thus improving security. Furthermore, the CSCF recognises practical differences in infrastructure implementations of SWIFT users. The CSCF is not a one-size-fits-all approach. Four architecture types are recognised which define the applicable controls and scope of components. Accordingly, SWIFT recommends that MAS a) takes a broader approach to cyber hygiene that covers technology, processes and people; b) defines a principle, objective and risk-based framework; and c) recognises the varying architectures and technology implementations of supervised institutions. <u>SWIFT leads the way on cyber hygiene</u> With near full adoption in 11,000+ SWIFT users, the SWIFT CSCF is now the established standard in cyber hygiene. Were the MAS to consider developing a framework similar to those outlined above, we would recommend that MAS might want build on this existing framework rather than start from scratch. <u>Monitoring approach</u> While recommendations on cyber hygiene practices are desirable, we believe MAS should also set out how it will monitor compliance of its guidelines. For example, the Notice could set out how entities will be expected to provide compliance acknowledgments to the regulator. To avoid

S/N	Respondent	Feedback from respondent
		overloading financial institutions' existing attestation processes, tools such as in SWIFT's CSP and KYC-Self Attestation service could be used.
40.	The Great Eastern Life Assurance Company Limited	**1. Comments on the applicability of the Notice:** Great Eastern does not have any comments on the applicability of the Notice. **2. Comments on the proposed definitions:** Please provide clarity if the term "administrative account" of the Notice is meant to be the same as: i) "privileged user" as described in paragraph 11.2 of the MAS Technology Risk Management Guidelines. ii) "system administrators" as defined under footnote 11 of the MAS Technology Risk Management Guidelines. It is noted that the definition of "system" differs slightly from that in the MAS 127 Notice on Technology Risk Management. MAS 127 defines system as part of an IT infrastructure, while the proposed definition does not. **3. Comments on the proposed cyber security requirements:** With reference to Paragraph 9(b) of the Notice, it would be good if the paragraph be clear on whether the confidential information referred means that owned by the relevant entity or encompasses those owned by third parties. For the latter, the relevant entity would not have any control on enforcing the use of multi-factor authentication. **4. Comments on the proposed transition period:** Great Eastern does not have any comments on the applicability of the proposed transition period. **5. General Comments:** Great Eastern does not have any general comments.
41.	Anonymous	Confidential
42.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Definition of "Multi-Factor Authenication" b. The definition for Multi-factor Authentication item (b) states that "something that the account holder has such as a cryptographic identification device or token." Need further clarification: In addition to cryptographic identification device or token, will SMS OTP or software token

S/N	Respondent	Feedback from respondent
		such as mobile apps OTP, i.e. Google Authenticator or vendor mobile apps OTP be considered as another factor of authentication? **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
43.	ICICI Bank Limited Singapore Branch	Confidential
44.	Securities Association of Singapore	Confidential
45.	Forcepoint Overseas Limited	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Administrative accounts Forcepoint recommends a risk adaptive protection approach to the security of administrative account holder. Risk adaptive protection approach is a strategy whereby an individual risks score is generated by monitoring and analysing the individual behaviour. This scoring is dynamically adjusted based on the type of activities. For example, if the individual's activities are corporate compliant, the risks score will be lower than an individual who is not corporate compliant. This scoring serves as a guide for dynamic and automatic implementation of security policies. The higher the score, the tighter the security measures. The lower the score, the company can relax on its security measure on the individual. The key benefits behind this dynamic scoring of a risk adaptive approach are as follows:

S/N	Respondent	Feedback from respondent
		- Prevention of insider threat - accidental or intentional. - Contain and mitigate compromised account by malware or hacker. - Detection, prevention and stopping data leakage. This strategy can be applied to individuals working on premise as well as off premise. This is especially important and useful in today's changing workforce working patterns. Security Patches 1) When a system is detected vulnerable, and a patch is not yet available, Forcepoint recommends virtual patching until the application patch is available and ready for that device. 2) Patches should be checked for malware. Forcepoint recommends the sanitisation of all patches to ensure that they are not compromised. Security Standards 1) Forcepoint recommends companies conduct periodic security assessment to determine their current security posture. The common assessment conducted usually includes vulnerability assessment and penetration testing. In view of the current threat landscape, company should also consider evasive malware testing. Today's malware is more sophisticated and advanced, and are often able to evade some of the current cyber security defences. 2) Dynamic risk adaptive protection as an extension of the discussion for administrative accounts described above, Forcepoint recommends that this strategy be implemented across the organisation. It is easier, cheaper and less risky to mitigate threats in its infancy than to manage and mitigate a fully blossomed breach. Additional benefits risk adaptive protection is implemented companywide. - Could potentially be used to develop a corporate aware security culture for the organisation. - Serves as notification for corrective cyber education for non-corporate compliant individuals. And when employees are able

S/N	Respondent	Feedback from respondent
		to recognise the face of threat, it strengthens the security posture of the company. An extension of this could lead to the implementation of an insider threat mitigation program. 3) Mitigating third-party threats by establishing a standard security posture within the banking ecosystem: The banking sector is experiencing an increased amount of collaboration between banks, suppliers and partners, working together to deliver a greater value to its customers. As a result, Forcepoint recommends that a baseline cyber security posture be implemented within the banking ecosystems to ensure that no one entity becomes a third-party threat to the other. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
46.	MSIG Insurance (Singapore) Pte. Ltd.	**1. Comments on the applicability of the Notice:** We note that it is intended that the proposed Notice shall apply to "any insurance intermediary registered or regulated under the Insurance Act". We would like clarification from MAS whether this includes "insurance agents" as opposed to "insurance brokers". The registration and licensing of "insurance agents" do not appear to come under the purview of the Insurance Act, although there are some regulated provisions in the Act applicable to them. If our interpretation is wrong and agents are to be included, does MAS expect a principal to be responsible for compliance of the proposed Notice by its agents? **2. Comments on the proposed definitions:** "confidential information" defined as "any information relating or belonging to the relevant entity that is not publicly available" in the draft Notice is pretty wide. Other than information published in a corporate website or document for public consumption, all other information on or belonging to a financial institution is not "publicly available". But not all such information is confidential to the extent that they need the highest level of protection.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: We are generally agreeable to the proposed cyber security requirements for financial institutions. However, if "insurance agents" are to be in scope, this will be very challenging for them, who come in all sizes and complexity. We also ask for clarification on the Multi-factor Authentication: in the phrase "access confidential information through the internet", what does this mean? If a system is accessed via VPN, it is considered as access through the internet. Is Multi-factor Authentication required for access via VPN? Are the requirements under this proposed Notice to apply to service providers or external systems used by a relevant entity? E.g. Office 365, systems used by outsourced service providers. Do they apply to organisations of which the relevant entity is a member? E.g. GIA and the outsourced systems used by GIA. Antivirus is not available on some type of on non-Windows systems. Can we clarify if this proposed Notice is applicable to these systems as well (e.g. telephone systems)? **4. Comments on the proposed transition period:** The Authority will need to consider financial institutions' budget and planning as IT enhancements and controls may require substantial investment. Sourcing for the appropriate IT solutions, fixing defects, testing and the whole suite of implementation may also take time. **5. General Comments:** No comments .
47.	Prudential Assurance Company Singapore (Pte) Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Confidential information –> (b) any information relating or belonging to the relevant entity that is not publicly available – To broadly classify anything not publicly available for corporate information as Confidential and to treat and protect them as such may be an overkill. System - If systems are broadly defined as in section 2, some of the security requirements may not be applicable or feasible to be applied on some of the system types like IP CCTV, projectors etc.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: *6. Security Standards* There are no security standards for all system types especially where "System" is defined as any hardware, software, network, or other information technology ("IT") component. i.e. Printers, IP CCTV, projectors, IoTs etc will not have any such standards readily available and be very much dependent on product vendor *8. Antivirus* Not all systems allow antivirus to be installed on them. We would suggest it to be worded more realistically *9. Multifactor Authentication* Not all system supports and integrate with MFA solutions. Will alternatives like jumphosts with MFA satisfy this requirement? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** What about third parties that we engage? Do they need to abide by this notice?
48.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** The definition of "Confidential information" needs to be defined further. The fact that information is not publicly available does not make the information confidential. We would propose that in relation to customer, confidential information is personal information of a customer which is not publicly available and in relation to an entity, it is confidential information which is not publicly available. Are the criteria to determine "Critical System" the same as those set out in the TRM Guidelines e.g. RTO of not more than 4 hours? Could a more risk-based approach to multi-factor authentication be taken? Compensating controls may be employed where multi-factor authentication is not feasible. The definition of "system" is too broad. If the term "system" is too broadly defined, the entity will face a lot of difficulties/challenges in complying with the notice. **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
49.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** “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; Please consider excluding anonymised, encrypted or tokenised information that is not referable to a named customer or an FI as part of the definition of confidential information. MAS guidelines on Outsourcing, “customer information” means – (a) in relation to an approved exchange, recognised market operator, approved clearing house and recognised clearing house, “user information” as defined in section 2 of the SFA; (b) in relation to a licensed trade repository and licensed foreign trade repository, “user information” and “transaction information” as defined in section 2 of the SFA; or (c) in the case of any other institution, information that relates to its customers and these include customers’ accounts, particulars, transaction details and dealings with the financial institutions, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred; **3. Comments on the proposed cyber security requirements:** • *Page 8, #9: Propose to review the use of Multiple Factor Authentication(“MFA”) based on the FI’s risk appetite and system capability for MFA. Certain legacy system may not be able to implement MFA, and there may be a “single point of failure”, if the FI is relying on a single MFA product to authenticate its system.*

S/N	Respondent	Feedback from respondent
		• *Page 8, #5(a) the security patch is to be applied within the timeframe which commensurate with the risks, according to the FI's risk appetite. This is to prevent the FI from making a security decision based solely on the Vendor's risk rating.* • *Page 11, Para-9: The statement mentions that the MFA is on operating System on critical system. This is misaligned from page 9, #9.* • *In relation to the requirement for anti-virus, would MAS consider carve-outs for Unix platforms where virus attacks are rare and non-critical intranet systems or generally a risk based approach towards the applicability of the bill?* **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
50.	Anonymous	Confidential
51.	Gartner Advisory Singapore Pte. Ltd.	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments, definitions look great! **3. Comments on the proposed cyber security requirements:** <u>Other Security Controls And Processes To Be Added</u> There are a few additional technology areas that represent foundational elements of a security program. Gartner feels FIs will benefit from having these in place and should be included in the proposed requirements (note: There needs to be an equal focus on associated processes to supplement these technologies – for example technical email security capabilities need to be enhanced with frequent user awareness training to combat phishing and business email compromise) *Email Security:* Relevant entities should have appropriate email security controls in place that provide anti-phishing, anti-spam, anti-malware and real time protection from malicious URLs. Additional recommended capabilities include business email compromise, digital rights management and data loss prevention for email messages. *Secure Web Gateway:* Relevant entities should have appropriate web security controls in place to protect users and the organization from browser

S/N	Respondent	Feedback from respondent
		based threats through URL filtering, advanced threat defence and legacy malware protection. These controls help organizations enforce internet policy compliance. *Security Monitoring and Response:* Relevant entity should have a 24/7 ability to detect and respond to threats. This could be through an in house security operations team or through leveraging a remote managed security service provider. A hybrid approach is also possible where an organization could utilize both approaches in tandem. (Note to MAS: It is important for MAS to clearly specify whether FIs are allowed to use MSSPs that transfer/stream security logs from the customer environment to their own SOC for analysis. If yes, does the data need to stay within Singapore? Many organizations have no choice but to use MSSPs for this type of capability due to the costs and skills shortages. Gartner clients are sometimes unclear about whether they can use MSSPs located outside of Singapore for these types of services or not) *Cloud Security:* Relevant entities adopting public cloud services should implement adaptive access control capabilities to ensure user behaviour is analysed in the context of identity and device context before granting access to cloud based resources. Relevant entities should demonstrate that they have effectively used native security controls offered by the cloud provider in conjunction with appropriate third party security controls to ensure they are addressing risks effectively. Comments on existing proposed requirements *5- Security Patching* 5 (a) – Relevant entities should prioritize vulnerability remediation not just based on severity of the vulnerability or criticality of the system but also by analysing if there is an actual exploit for that vulnerability currently in circulation. This can be done by correlating vulnerability assessment results with external threat intelligence. Gartner predicts that by 2022, organizations that use the risk-based vulnerability management method will suffer 80% less breaches. 5 (b) – Relevant entity must institute compensating controls in the same timeframe that it would normally remediate the identified vulnerability. *6 – Security Standards*

S/N	Respondent	Feedback from respondent
		Security standards should focus on hardening systems to reduce risk and by managing access to other 'systems' on the principle of least privilege (i.e. only give systems access to resources they absolutely need) *8- Antivirus* Relevant entities should supplement anti-virus technologies (i.e. those that detect known malware) with endpoint detection and response [EDR] capabilities for highly sensitive endpoints handling confidential information. EDR focusses on detecting malicious behaviours and enabling remediation and response activities on endpoints to prevent spread of attackers laterally within the environment. *9 – Multi-factor authentication* For administrator accounts, relevant entities MUST NOT use Out of Band SMS (i.e. SMS based One Time Password) methods as a MFA method. OOB SMS has proven to be vulnerable to carrier based (SS7) and malware attacks, both of which have been successful. For administrator accounts, only mobile push and OTP hardware tokens should be used. **4. Comments on the proposed transition period:** 18 months is probably fair, especially considering that there are several processes that need to go hand in hand with the technology implementations. Also, creating internal capabilities for security operations can take at least 18 months. One idea may be to put the 'low hanging fruit' like firewalls, AV, patching, email security, web security, MFA on a 12 month timeframe and the more resource intensive elements like security standards and security operations on an 18 month timeframe. **5. General Comments:** These are welcome steps and thank you for the opportunity to comment. Generally, CISOs need to be mindful that their traditional notions of controlling data by locking it down physically within the datacentre have to change. To succeed in digital business, FIs need to share data within the organization and externally with customers, partners. So, the idea should be to effectively move security policy with the data and with the context of the end user rather than making security and access control a one time gating decision.
52.	Anonymous	Confidential
53.	Anonymous	Confidential
54.	Oracle	**1. Comments on the applicability of the Notice:**

S/N	Respondent	Feedback from respondent
		Oracle agrees on the need to establish a waterline that covers all entity types within the financial sector, across banking, insurance, capital markets, etc. However, as MAS would appreciate, the resources available to a large-scale commercial and retail bank will be substantially different to those available to smaller institutions, including those in the emerging FinTech space. Although the suggested waterline may be appropriate for these smaller institutions, we would suggest that larger organisations within this sector may benefit from a stricter set of mandates (i.e. a higher waterline). This approach would not be dissimilar to the ranking of merchants (according to transactions per year – although the metric could be different in MAS's case) into "merchant levels" within the PCI-DSS standard. This type of ranking recognizes that the resources available to properly ensure Cyber Hygiene are different amongst organisations of differing sizes, and is concomitant with the fact that larger organisations typically represent a more attractive target for adversaries. **2. Comments on the proposed definitions:** Our sole comment on the proposed definitions relates to the term "system". We would propose that rather than use this term to denote a component of software and/or infrastructure (e.g. firewall, router), that the definitions of "component" and "system" are cleanly segregated, the latter being used to refer to a collection of "components" whose collective purpose is to gather and/or source information (confidential or public) from/to individuals and/or other "systems". Such a definition would be more in-line with the earlier definition (or sub-type) of "critical system". **3. Comments on the proposed cyber security requirements:** (5) Security Patches With respect to the application of security patches, we commend MAS on including this as a priority. Being cognisant of the operational difficulty of staying current with vendor-provided patches, we would suggest that this requirement is slightly augmented. It is well-known within the cybersecurity sector that one of the most productive actions that can be taken by any organisation is to patch those vulnerabilities for which a known exploit exists. Known vulnerabilities (without known exploits) are important to patch, but the priority should be afforded to the former category, given the resources that this activity will require of the impacted organisation.

S/N	Respondent	Feedback from respondent
		With this approach in mind it may be appropriate, at a national level, to provide threat intelligence to the financial sector that is delineated in such a fashion. This would greatly assist organisations in mitigating their risk of a data breach or threats to business continuity. Allied with this, we believe entities within the financial sector should investigate, where possible, the use of "components" that are self-patching in this regard i.e.the patching of vulnerabilities is essentially outsourced to a 3rd party – this may help to obviate the practical difficulty and operational impact on organisations attempting to continually patch their own systems. 9) Multi-Factor Authentication We welcome the suggestion to use MFA in respect to administrative accounts. However, it should be clear that this approach is primarily useful in mitigating the risk of malware-initiated logins (i.e. instituted by some remote adversary) to administrative accounts. It is less useful in terms of dealing with insider threats (which may originate with administrative users or end-users). To address this requirement, we would suggest that the following two controls are required: (a) Segregation of Duties for Administrative Users This would entail the application of preventive controls to ensure Administrative accounts have the privilege to execute their functions, but without access to confidential data. Technologies to achieve this are quite mature (and were largely motivated by the Sarbannes-Oxley regime in the US) (b) Auditing/Monitoring of Administrative and End Users This is a principally detective approach. Detection of user activity is a critical component of good cyber hygiene. We note that the RBI (Reserve Bank of India) strongly recommends that banks within their jurisdiction implement some form of access monitoring to core banking systems. We would suggest that MAS consider similar. As per our response to Section 1, it may be that this approach ((a) and (b)) is mandated only for those larger organisations that are equipped to implement such controls. **4. Comments on the proposed transition period:** We believe the proposed transition period of 12 months is appropriate.

S/N	Respondent	Feedback from respondent
		5. General Comments: Oracle welcomes this initiative by MAS to raise the overall level of Cyber Hygiene amongst organisations operating within Singapore's financial sector. We believe that it is a good first step towards securing a critical part of the nation's cyber infrastructure
55.	Finexis Asset Management Pte. Ltd.	**1. Comments on the applicability of the Notice:** We are not sure whether exempt financial advisers are included in the list. If they are not, we would suggest including them in the list. **2. Comments on the proposed definitions:** 1) The paper has stated that "administrative account", in relation to a system, means any user account that has full privileges and unrestricted access to the system; Will there be a situation whereby the administrative account could only assign types of access to users, eg, "View only", "View and Edit", etc. If that is the case, should this definition be modified? 2) The paper has stated that "confidential information" means — …. (b) any information relating or belonging to the relevant entity that is not publicly available;" This definition could be too broad to cover many categories of information. For example, an information may be only be known to the entity only. But even if it is "leaked" to parties outside the entities, it has no material impact at all. Suggest to amend it somewhat to exclude trivial information that is only available to the entity. **3. Comments on the proposed cyber security requirements:** The requirements are good practice for cyber security. Our concern is cost of implementation. Many RFMCs are struggling to survive given the market conditions and keen competition. Given the various escalating costs related to compliance, IA, IT systems, office rental, labour, etc, any additional costs will affect the financials of RFMCs further. Please consider this aspect when introducing the new regulations. **4. Comments on the proposed transition period:** 12 months is a good timeframe **5. General Comments:**

S/N	Respondent	Feedback from respondent
		No comments.
56.	HITRUST Alliance (“HITRUST”)	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** While the proposed Cyber Hygiene Practices enumerated in the draft Consultation Paper are certainly necessary, they are by no means sufficient for the reduction of cyber risk faced by financial institutions in today’s threat environment. The proposed measures focus on technical controls and do not address administrative or physical controls that must also be implemented to help ensure good cybersecurity. The technical measures also do not provide enough information to ensure the good security hygiene the Monetary Authority seeks. For example, the measures for Para 6 – Security Standards do not specify the breadth of the standards needed nor the depth of their prescription. This leaves the implementation of these measures open to interpretation, which will result in widely varying degrees of protection that organizations would actually afford sensitive financial information. **4. Comments on the proposed transition period:** Given their basic nature, we believe financial institutes are likely already implementing these good cyber hygiene practices and only a very limited—if any—transition period would be necessary. **5. General Comments:** HITRUST applauds the efforts of the Monetary Authority of Singapore to establish minimum good cybersecurity hygiene requirements for the financial entities listed in the draft but believes a broader range of good cyber hygiene practices and more prescriptive measures supporting these practices is necessary before the Monetary Authority can achieve its objectives for this guidance. HITRUST recommends the adoption of a more comprehensive controls framework-based approach that is easily consumed by any organization, internationally and regardless of industry, such as the HITRUST CSF, which is based on ISO/IEC 27001/2 and incorporates and harmonizes multiple standards and best practice frameworks, including the EU GDPR and Singapore PDPA. We also believe that a robust approach to cybersecurity also includes the ability to exchange standardized assurances from independent third-parties about one’s

S/N	Respondent	Feedback from respondent
		cybersecurity program with other entities, such as business partners, customers and regulators.
57.	Anonymous	Confidential
58.	SingCash Pte Ltd Telecom Equipment Pte Ltd (Collectively known as "Singtel")	**1. Comments on the applicability of the Notice:** (a) Relevant Entities under Proposed Payment Services Bill • Singtel notes that the list of relevant entities are fairly exhaustive but we note that the MAS intends to include even licensees under the Proposed Payment Services Bill. • It may be premature for the MAS to cover entities that may be covered under a proposed legislation. We note that the last time the MAS consulted on the proposed Bill was January 2018 where it outlined proposed licensee categories. No decision has been made yet. Given the significance of the proposed Bill, we do not believe that it is advisable for the MAS to apply the Notice, potentially, on entities that may or may not be subject to the Bill. • Nonetheless, we note that all entities who own critical information infrastructure in Singapore must already comply with the requirements of the Cyber Security Act. This will mean that the bulk of the intended licensees for this Notice will in fact already be compliant with the Cyber Security Act and there is therefore less urgency for the MAS to impose these requirements on any entity that may be covered under the proposed Bill. • At the same time, the MAS may wish to reconsider application of the requirements on all FIs, regardless of size. Many of the intended relevant entities may be small in set up and compliance with the requirements will attract higher costs. (b) Telecommunication licensees offering limited e-money services • We note that the MAS proposed Payment Services Bill states that limited e-money services will be excluded from the ambit of the proposed Bill. In our response to the MAS on 8 Jan 2018, we had supported this on grounds that this will correspond with the current set of single purpose stored-value facilities (SVFs) where the SVF used to pay for goods and services offered by the SVF holder itself. • Prepaid mobile stored value facilities offered by mobile telcos today are considered single purpose SVFs and therefore, should correspondingly be considered limited e-money services and be excluded from the proposed Notice too. • Notwithstanding this, we do believe that telecommunication licensees who are considered Critical Information Infrastructure owners (CIIOs) under the Cyber Security Act should also be excluded from the Notice on

S/N	Respondent	Feedback from respondent
		grounds that (i) any SVF they offer will be limited e-money in nature and (ii) they are automatically covered under the Cyber Security Act **2. Comments on the proposed definitions:** We have the following comments (a) Multi Factor Authentication • the MAS proposed definition limits the type of authentication methods (b) System • the MAS proposed definition does not address the issue of where an entity's systems do not all belong or are under the operational control of the entity. We elaborate on these in Question 3. (c) Administrator vs administrative account – an administrative account, in relation to a system, should mean a user account that performs administrative tasks, such as user creation, password reset, etc. Administrator account, in relation to a system, means a user account that has full privileges and unrestricted access to the system. (d) Confidential Information – the MAS has limited this to largely publicly available information. There could be non-confidential information that may not be publicly available. In typical non-disclosure agreements, parties involved in handling of information will rely on the owner of the information to determine whether the information is or is not confidential. We believe this a more reasonable definition to use. **3. Comments on the proposed cyber security requirements:** (a) There is the presumption that the relevant entity is able to control the kind of security requirements on all systems that it uses or has to access. In many cases, entities do not use their own systems, eg their HR systems could be outsourced. Therefore, it is not practicable for the entities to require that all these systems be subject to multi-factor authentication. We therefore propose that the Notice applies to the critical systems of the relevant entity, ie all the Cyber Hygiene practices will therefore apply to the critical systems instead of broadly covering systems. (b) In terms of security patches, we believe it is reasonable to caveat that a relevant entity should apply these once it is aware of the vulnerability. This is because there will be many

S/N	Respondent	Feedback from respondent
		cases where the entity may not be aware and to specify it will mean reduce the burden of dispute and argument over whether a relevant entity has complied with requirements of the Notice. (c) In terms of multi factor authentication, first, we refer the MAS to our views on the scope of 'systems' used. Secondly, we note that the definition and requirements of multi-factor authentication will be far too burdensome, eg requiring either token or cryptographic identification device. Many entities today rely on 2 factors with the second largely being an SMS-OTP. To institute the multi factor authentication will be far too difficult. we propose allowing entities to continue with their form of multi factor authentication as long as they have carried out their risk assessment and concluded that the form of authentication they use meets their requirements. (d) Firewall(s) to be implemented : In the DMZ (De-militarized Zone) with 2-tier firewalls, the Internet-facing firewall allows network traffic coming from Internet. It is difficult to determine whether the network traffic is authorised or unauthorised. However, the second firewall is configured to accept network traffic from its own servers in the DMZ. (e) Anti-virus measures to be implemented. We believe that it is more appropriate to require that a relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system, where anti-virus or malware software is available. **4. Comments on the proposed transition period:** • We believe that the proposed transition period should be at least 12 months from the effective date and up to a period of 18 months. **5. General Comments:** • The MAS has not provided any clarity or information on the legal effect of the proposed Notice, eg (i) will it become a form of subsidiary legislation (ii) the penalties for non-compliance etc • Where the MAS intends that these are voluntary practices, we believe it is necessary to make this known too.
59.	St. James's Place International	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:**

S/N	Respondent	Feedback from respondent
	plc (Singapore Branch) St. James's Place (Singapore) Private Limited	In view of the proposed definition of "system", we are of the view that, instead of the term "administrative account", the term "system administrative account" appears to be a better representation of the proposed definition. **3. Comments on the proposed cyber security requirements:** Whilst the intent for multi-factor authentication (MFA) is good, it may not be feasible on certain systems due to their technical limitations. More often than not, such systems are hard-coded or utilise a local authentication database which do not support MFA. In view hereof, we propose for a more practical and balanced approach to be taken, i.e. MFA be implemented where possible. In relation to the proposed requirement to apply security patches to address vulnerabilities, we are of the view that it would be useful for MAS to refer FIs to a vulnerability scoring and assessment framework such as the Common Vulnerability Scoring System (CVSS). This enables FIs to prioritise their corrective actions according to the severity of threats. In addition, we would like to understand if MAS would view every FI differently in terms of the implementation of the 6 cyber hygiene requirements? The reason is that every FI differs in scale, complexity and nature. It is onerous to expect an FI to implement the same standards/degree of controls of a large FI. **4. Comments on the proposed transition period:** The 12 months transition period may be insufficient for FIs to comply with the proposed requirements if significant investment and resources are required. Hence, we propose a period of 18 months. **5. General Comments:** We welcome MAS' intention to prescribe a set of essential cyber security practices that Financial Institutions (FIs) must implement to manage cyber threats and strengthen the overall cyber resilience of FIs
60.	Anonymous	Confidential
61.	Schroder Investment Management (Singapore) Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		Security Patches We would like to highlight that there could be situations whereby the application of security patches would cause the application to break or render the vendor not being able to support the application, which would impact relevant entity's operations. Due to such limitations, we would like to request the Authority to consider the provision of an option in the Notice to allow relevant entities to institute appropriate controls to reduce any risk posed for not applying the security patches to its system in the cases where the security patch cannot be applied to the system due to system malfunction or invalid vendor warranty support. Security Standards We note that there are systems which (a) might not have industry security standards or (b) security standards are not provided by the relevant vendors. In view of this, we would like the Authority to consider amending the definition of "security standards" to "in relation to a system, means a set of configurations OR and procedures for the purpose of safeguarding and improving the security of the system". This would provide flexibility to relevant entities to implement appropriate controls and procedures where security standards are not available. Anti-virus There could be situations whereby installing anti-virus (a) would break the application due to performance issues that will impact relevant entities' operations or (b) is ineffective when installed on Linux/Unix variants operating systems. As such, we would like to request the Authority to consider the provision of an option in the Notice to allow relevant entities to institute appropriate controls to reduce any risks posed for not implementing anti-virus on the system in situations where anti-virus cannot be implemented on the system as it may result in system malfunction, or non-effectiveness (e.g. Linux, Unix variants of operating system). Multi-Factor Authentication (MFA) With the vast spectrum of type of institutions in the financial industry which have varying business nature, size, complexity and IT capabilities, we would like to highlight that there might practical challenges faced by relevant entities if this MFA requirement is stipulated as compulsory in the Notice. Thus, we would like to seek the Authority to re-consider whether MFA requirements should be imposed across all relevant entities or only to certain types of financial institutions.

<table>
<tr><th>S/N</th><th>Respondent</th><th>Feedback from respondent</th></tr>
<tr><td></td><td></td><td>
<p>Alternatively, the Authority may wish to consider the provision of option in the Notice to allow relevant entities to institute appropriate controls to reduce any risk posed for not implementing MFA on applications in situations where the relevant entity has assessed it not to be cost effective or the implementation is too complex, on a risk based approach.</p>
<p><b>4. Comments on the proposed transition period:</b>
We would like to propose a tiered approach for transition period as set out below:-</p>
<table>
<tr><th>Cyber Hygiene Requirement</th><th>Transition Timeline</th></tr>
<tr><td><ul><li>Administrative Accounts</li><li>Security Patch</li><li>Security Standards</li><li>Firewall</li><li>Anti-virus</li></ul></td><td>12 months</td></tr>
<tr><td><ul><li>Multi-Factor Authentication</li></ul></td><td>24 months
Reasons:<ul><li>Relevant entities might not have this technology in-house currently and would need to source for the most appropriate software/ provider;</li><li>Relevant entities would need time to engage with their outsourced service providers i.e. HR payroll vendors, system vendors etc. which are impacted by this requirement and work out a feasible resolution.</li></ul></td></tr>
</table>
<p><b>5. General Comments:</b>
We understand that the relevant entities are responsible and accountable for all services outsourced to providers regardless of where they are located / incorporated. Hence, we would like to seek the understanding of the Authority to allow relevant entities the
flexibility to institute appropriate controls to mitigate any risk posed in the event that such Notice cannot be applied extra-territorially or on providers who do not fall under the definition of the relevant entities.</p>
</td></tr>
<tr><td>62.</td><td>Insmart Insurance Agency Pte LTd</td><td>
<p><b>1. Comments on the applicability of the Notice:</b>
We support the initiative as proposed.</p>
<p><b>2. Comments on the proposed definitions:</b>
The proposed definition is clear.</p>
<p><b>3. Comments on the proposed cyber security requirements:</b>
The security requirement is acceptable.</p>
<p><b>4. Comments on the proposed transition period</b>
The one-year transition period is acceptable.</p>
</td></tr>
</table>

S/N	Respondent	Feedback from respondent
		5. General Comments: No comments.
63.	Allianz Global Investors Singapore	**1. Comments on the applicability of the Notice:** No further comments. **2. Comments on the proposed definitions:** - "System": The definition appears broad when viewed from an implementation perspective (e.g. on hardware front). For us to get a sense of the scope, can the MAS please provide examples. - "Vulnerabilities": We suggest MAS to only consider for "published" weakness, susceptibility or flaw of the system, as it will help us to prioritise the remediation of vulnerabilities. **3. Comments on the proposed cyber security requirements:** No further comments. **4. Comments on the proposed transition period:** No further comments. **5. General Comments:** No further comments.
64.	DP Credit Bureau Pte. Ltd.	**1. Comments on the applicability of the Notice:** DP Credit Bureau agrees that licensed credit bureau under the Credit Bureau Act 2016 should be included into the Notice. **2. Comments on the proposed definitions:** DP Credit Bureau is comfortable with the proposed definitions. **3. Comments on the proposed cyber security requirements:** DP Credit Bureau finds the proposed cyber security requirements are relevant and could effectively safe guard its credit bureau data against cyber threat. **4. Comments on the proposed transition period:** DP Credit Bureau finds the proposed transition period is sufficient. **5. General Comments:** In general, DP Credit Bureau supports the issuance of this Notice of Cyber Hygiene.
65.	Anonymous	Confidential
66.	Anonymous	Confidential

S/N	Respondent	Feedback from respondent
67.	Aetna Insurance Brokers	**1. Comments on the applicability of the Notice:** Agree. **2. Comments on the proposed definitions:** Sufficiently clear and suitable. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** Timeframe is sufficient. **5. General Comments:** No comments.
68.	Control Risks	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** Control Risks welcomes the move by the Monetary Authority of Singapore to improve the resilience of the Singapore's financial services sector. Singapore has been a global leader in ensuring the security of a nation's information systems, and this latest program consolidates that position. The approach set out is strong and will encourage the use of some of the global finance industry's best practices. However, prescriptive technology requirements often lead to a focus on compliance rather than security goals. At Control Risks, we have worked with a number of regulators and supervisory authorities across the world to develop and implement a threat led and risk-based approach to cyber security and critical infrastructure resilience, and we believe that such an approach for Singapore's financial services would promote an even more resilient sector.

S/N	Respondent	Feedback from respondent
		Threat led approaches to industry-wide cyber resilience are best exemplified by the Bank of England's CBEST framework. But they are now being adopted by a number of other regulators across different jurisdictions and sectors, including Hong Kong's iCAST, the Netherlands' TIBER-NL and the broader European Union's TIBER-EU frameworks. Threat led resilience testing leverages up-to-date and accurate threat intelligence, collected and analysed in a legal and ethical way in order to test the resilience of critical functions and systems underpinning the financial sector in a country in light of the actual threats that it faces. The focus on intelligence-led testing against live critical systems provides a clear understanding for the regulator as well as each participating financial institution of its own and the broader sector's resilience to advanced cyber attacks. In addition, leveraging real threat intelligence and testing on live critical systems through cooperation between suppliers, financial institutions and regulatory authorities promotes cooperation across all actors involved in ensuring the resilience of critical financial infrastructure. The benefits of a threat led approach include the following: • A more granular understanding of the specific threat actors that can target a sector and the specific actors within that industry, their role as part of critical infrastructure and importantly the key systems that underpin this infrastructure, enabling the development of realistic testing scenarios and an assessment of the overall resilience of each institution and the broader sector. • A more effective allocation of resources to meet the threats identified, as the institution can develop responses specific to its own threats and those faced by its own critical systems, rather than those that are relevant to a large number of institutions (and hence may not be strictly relevant) • A higher return on an institution's investment in cyber security, as finite resources are not expended on assets that are of low priority, or to defend against threats that are not relevant to the institution. • A stronger 'buy-in' from institutional stakeholders as they perceive that their cyber security program meets 'real-world' threats, rather than simply managing to meet a set of compliance standards that can appear to be abstract.

S/N	Respondent	Feedback from respondent
		• It establishes a baseline threat environment, which institutions can then develop their threat responses as the threat environment changes in response to technological, geo-political and social changes. • An ability to coordinate more effectively with other regulators (such as the Bank of England) who are using a threat led approach The main challenge to instituting a threat led approach is to ensure appropriate collaboration between all stakeholders involved in the development of such frameworks. In our experience at Control Risks a collaborative approach, involving regulators, the supplier community and most critically the participating financial institutions, can lead to an effective implementation of a threat-led resiliency framework.
69.	AL Wealth Partners Pte Ltd	**1. Comments on the applicability of the Notice:** <In general, some of the "hardening" recommendations as currently defined will create inefficiencies, increase costs and impact overall productivity as it does not seem to allow FIs to "tailor/right-size" the requirements according to their business risks. If the notice is applicable strictly to the entity and its physical on-site systems, it may be possible for entities to comply with most but not all of the requirements being recommended, but if the requirements are imposed even on third party providers and additionally on entities' employees who work from home through remote access or who have access through their own devices (e.g. mobile phones/ipads/home pc), SME FIs' ability to comply will be significantly impaired. The expected cost of implementing the controls being proposed are an impediment as FIs would need to incur expenses for additional monitoring software and also physical hardware for their employees who are given remote access. Companies may reconsider allowing flexi-place arrangements to control costs which is going against the drive to improve work-life balance. • The universe appears to be too wide to be practicable. It is not just the money concerned but also the implication to "reverse or inhibit" those other initiatives these companies have implemented as promoted by the Government. **2. Comments on the proposed definitions:** <Most of the definitions are the same as that found in the TRM except for the following which we think may need to be revisited.

S/N	Respondent	Feedback from respondent
		The definition of Systems is too wide and vague as it now includes any device that is connected to the company’s IT infrastructure e.g. includes home PCs and personal devices. MAS expects companies to manage, check, mitigate, patch etc all devices in a timely manner. Does MAS have a definition for “timeliness” e.g. will FIs be given time to test patches before allowing them to go live in our systems? Will MAS issue patching standards which we should follow e.g. software has CIS but hardware has no industrial standard. Will MAS expect all personal devices to be included? The revised definition of Confidential Information (which now includes company’s own employees’ data and internal policies and procedures since these are not publicly available) could mean that FIs would need to revisit their definition of Critical Systems as the TRM definition only required FIs to consider systems that captured client data. • With a wider scope, it might mean ALL employees who work remotely will need multi-factor authentication (is 2-way authentication sufficient?). > **3. Comments on the proposed cyber security requirements:** <While we appreciate that more controls should be implemented to safe guard the IT systems, the way the draft Notice is written, we think the hardening standards may not be practicable without incurring significant resources and costs as we may need to restructure and make acquisitions of new equipment etc > With the withdrawal of PIC, this means most of the corporations which are below the size of MNC will likely unable to shoulder such sudden increase of IT cost amongst many other costs like compliance, human resources etc. **4. Comments on the proposed transition period:** <If MAS expects all the requirements to be implemented, 12 months is insufficient as the industry and many service providers are not ready. Despite Technology supposed to help speeding up things and provide efficiency in getting things done, from what we all experience and know, to get an IT system or software to be implemented and workable, it takes much longer than all Technology can put together and the cost in terms of manpower and real actual money spent can be enormous. These vendors will just find another way to charge huge amount of monies to those who are “obliged” by regulator to buy their service which to the user companies, many of such systems who claim to do the job, may end up no difference than those untested ones. Money spent cannot be recuperated whilst they remain unable to fulfil the regulator’s expectation or

S/N	Respondent	Feedback from respondent
		requirement, not a Win-win-Win situation. Reaction to recent incidents to try to plug the gap fast is not the real solution to the problem, there needs to have a well thought-out plan and action guidelines to ensure the good intended regulations are effective and long lasting.> **5. General Comments:** As mentioned, we agree that good Cyber Hygiene standards are essential but the rules should not be so rigid to the extent that companies' productivity would be impaired and contradicts to the Government wide initiatives and drives to provide a "work-life-balance" "flexi-work" environment by employing technology to facilitate such. There must be a workable solution to balance both. It would help, if MAS intends to draw up with great clarity and a fixed set of expectations more prescriptive requirements would be appreciated (e.g. define timelines, standards etc)
70.	Anonymous	Confidential
71.	Gemalto, Enterprise & Cybersecurity BU	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Additional measures proposed to enhance Para 4 - Administrative Accounts • As more digital assets are moving to the cloud and are increasingly being managed by third-party IT administrators, relevant entities should enact a separation of duties policy to prevent insider attacks. Such a policy allows administrators to perform administrative tasks – such as managing file servers or databases – without having access to information contained in those files. • Relevant entities should also implement the M of N control policy to administrative functions of critical resources to prevent a single administrator from making unauthorised changes. Additional measures proposed to enhance Para 6 - Security Standards • With the rise of connected devices/IoT, the relevant entity should ensure that they adopt the right authentication methods to address machine-to-machine or application-to-application transactions. Instead of applying multi-factor authentication on them, these cyber elements can be more reliably identified by their Digital Identities (Private Keys)

S/N	Respondent	Feedback from respondent
		and Digital Signatures. For example, the entity should verify a HTTPS site's SSL keys/certificate before establishing a secure session with the website. Given their impact on cybersecurity, hosting those digital identities and signatures in secure and tamper-proof hardware should be considered as one of the basic cyber hygiene requirements. • Furthermore, the digital signatures of the cyber elements should be periodically checked to ensure that nothing has been changed unknowingly. This will prevent situations in which cyber elements are replaced with unauthorised one(s), causing the entire business and security logic to be bypassed. <u>Additional measures proposed to enhance Para 9 - Multi-factor Authentication</u> • To enhance the effectiveness of multi-factor authentication, a relevant entity should adopt risk-based authentication, which uses continuous passive behavioral biometrics and context-based signals (such as geolocation) to accurately analyse the authenticity of any transaction in real time. This enables the entity to build a multi-dimensional profile of each individual end-user and strengthen their identity and access management, which is crucial when it comes to securing administrative accounts of critical systems. <u>Other additional measures proposed</u> As entities embrace virtualization, cloud and mobility technologies, they need to take a data-centric approach to safeguarding their sensitive data. They should encrypt their sensitive data – both in motion and at rest – to ensure that the information remains secure no matter they are – be it in databases, applications, storage systems, virtualized platforms, or cloud environments. • To protect data at rest, entities should use a tokenization solution which replaces sensitive data with a unique token (i.e. surrogate value) that is stored, processed or transmitted in place of that data. For entities that have a large scale, distributed environments, they can consider using algorithm-based (also known as vaultless) tokenization solution that offers high performance and scalability. They should also apply granular access controls to ensure that only authorized users or applications can decrypt and view sensitive data. • As for data in motion, entities should leverage network encryption devices that deliver data encryption capabilities

S/N	Respondent	Feedback from respondent
		with minimal latency to secure data without compromising network performance. • Also to safely dispose sensitive electronic records, entities should adopt digital shredding, which involves encrypting the data to dispose of it. This is essential, especially since other methods such as physical destruction, degaussing and overwriting, are not fully applicable to cloud computing. <u>Crypto key lifecycle management</u> • Entities ought to have hardware security modules (HSMs), which are dedicated crypto processors that are specifically designed for crypto key lifecycle management. • HSMs should pass the laboratory test under the Cryptographic Module Validation Program (CMVP) of the US National Institute for Standards and Technology NIST. HSM are validated as conforming to FIPS 140-1 and FIPS 140-2, are accepted by the Federal Agencies of Canada and USA for the protection of sensitive information and are accompanied by documentation bearing the FIPS logo of approval. • HSMs excel at securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications. • With FIPS-validated and NIST-approved HSMs, entities will be able to better protect transactions, identities, and applications as well as meet audit requirements since all cryptographic operations occur within the HSM and the keys never leave the hardware. HSMs also enable entities to address compliance requirements such as PCI DSS. • Entities must also remain in control of all their cryptographic keys used for encrypting and decrypting sensitive data, in order to protect that data throughout its lifecycle. This calls for the ability to streamline encryption deployment, as well as centralise policy and key management across the enterprise. To further reduce the chances of data loss, relevant entities should also limit access to cryptographic keys by enacting a separation of duties policy. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** Entities are increasingly adopting hybrid cloud to not only improve efficiency and productivity, but also provide better customer experiences. With data being stored and constantly moving across various environments – be it on-premise, public

S/N	Respondent	Feedback from respondent
		cloud or private cloud – to achieve those goals, data ownership is becoming a grey area. Banks should therefore leverage encryption and cloud-agnostic full lifecycle keys management solutions to regain full ownership of their data security. Such solutions will enable them to securely manage and store sensitive data and cryptographic keys, as well as ensure they can best manage and control user access, to effectively prepare themselves for a breach. To further strengthen their security posture while providing convenience to end users, relevant entities should also look at ways to work with the public sector. For instance, they could use the upcoming National Digital Identity (NDI) system in Singapore to onboard new customers. This not only simplifies customer identity management but also limits the risk of ID theft and fraud.
72.	Stradegi Consulting Pte. Ltd.	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** “Administrative account” is currently defined as any user account that has full privileges and restricted access to the system. We kindly seek further clarification on the term “full privileges and restricted access” to avoid misinterpretation. Does it predominantly entail system administrators having complete access rights to the systems which includes setup of access and user rights (read/write), functionalities, visibility of certain portfolios, entities, etc.? Ordinary system users who are just assigned to use the system in accordance with the internal procedures and technical restrictions are conversely excluded from this definition. Will the notice be solely applicable to administrative user accounts residing in Singapore and not cover external administrative accounts? In matrix organisational structures the administrative account is often located at headquarters outside Singapore. The definitions of “critical system” and “system” are identical with definitions in the Notice on Technology Risk Management for which a recovery time objective (“RTO”) is foreseen to be not more than 4 hours for each critical system. For clarification purposes refer to this notice. Few of the definitions in addition to the Cyber Hygiene Practices refer to the term “relevant entity”. This term is not defined in this drafted notice and can leave room for interpretations, in terms of local versus regional versus global entities.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: In general, can identified administrative accounts be secured centrally and at a higher level of access, i.e. for instance rolling out a multi-factor authentication for logging into the PC at start of the day instead of having a multi-factor authentication per system? Paragraph 7: In organisations where the Headquarters including IT support resides outside Singapore, firewalls are often implemented centrally covering all subsidiaries and branches. We kindly seek clarification whether this would suffice. Paragraph 9: Multi-factor authentication for all accounts on any system used to access confidential information through the internet is very broadly formulated in combination with the definition of "confidential information", as well as the addition "through the internet". Annex B gives an example of remote access to staff information through the internet. Nowadays a lot of companies enable their employees for remote access to all necessary systems as part of their business continuity plan. Is the intention of paragraph 9b) to have a multi-factor authentication in place for the login to remote access whereby confidential information can be retrieved? It will be beneficial to define either that solely remote access is meant or otherwise to clarify the term "through the internet" keeping in mind that most companies make use of cloud services whereby any non-public data is stored and retrieved via the internet. This would make it impractical to foresee each and every system containing non-public data with a multi-factor authentication. **4. Comments on the proposed transition period:** We believe an implementation period of 12 months is adequate. **5. General Comments:** Annex B – Paragraph 9: Another example would be remote access to client information which is non-public and stored in CRM systems.
73.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** My comment is with regards to the need to implement multifactor authentication as spelled out in Para 9. We need

S/N	Respondent	Feedback from respondent
		more clarity on whether multifactor authentication is still required in cases where system(s) on the cloud can only be accessed via white labelled IP address (or addresses) and with TCP/IP handshake in place. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
74.	VISA	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** As one of the leading global payments technology company, Visa welcomes the opportunity to contribute to the Notice on Cyber Hygiene consultation paper and appreciates the significant efforts driven by the Monetary Authority of Singapore (MAS) to strengthen cyber resilience in Singapore. Visa supports the approach to cyber security taken by MAS based on a commitment to fair and open competition, promoting global best practices and ensuring a flexible, risk-based approach to cyber security. We welcome and support MAS's effort to develop wide industry standards of cyber hygiene in a holistic, transparent and easily comprehensible manner, with the objective to encourage wider adoption of e-payments in Singapore.
75.	Industrial & Commercial Bank of China Limited	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** 1. Regarding the timeline requirement of applying security patches into its system when there is any security patch available, ICBC Singapore Branch is already following a process

S/N	Respondent	Feedback from respondent
		of updating our system with security patches. When a security patch becomes available, ICBC Head Office performs an analysis of the system vulnerabilities to be addressed by the patch and an assessment of the risk posed by the vulnerabilities. The priority of applying the patch into system depends on the risk assessment results. Any available security patch has to be updated successfully and tested to be able to address the system vulnerabilities in the testing environment before it can be applied into the production system. 2. Regarding the security standards, we seek clarification on whether the MAS has specific requirements or would MAS expect FIs to define and formalize those security standards on their own. **4. Comments on the proposed transition period:** 1. FIs may require more time to perform an assessment of the cyber hygiene of existing IT systems to allow for a better understanding of the existing cyber hygiene position and gaps to be covered. We respectfully propose for MAS to consider a transition period of 18 months. **5. General Comments:** 1. In view of growing threats in the cyber landscape, this Notice on Cyber Hygiene is very necessary and significant to guide FIs to further strengthen their overall cyber resilience. We look forward to more training seminars or forums for exchanges among FIs to be organized to facilitate the sharing of experiences and practices so as to collectively guard against cyber threats.
76.	Anonymous	Confidential
77.	Anonymous	Confidential
78.	RHT Compliance Solutions	**1. Comments on the applicability of the Notice:** The industry, in general, is supportive of MAS prescribing regulatory requirements on cyber hygiene measures for financial institutions' compliance. As the financial industry is a critical sector in Singapore's economy and is an attractive target for cyber-attackers, having cyber hygiene practices imposed on the financial institutions would enhance cyber security across the financial industry. We note that MAS has proposed a comprehensive list of FIs or relevant entities across the financial sector to whom the Notice will apply. However, it is unclear whether small insurance agents that are not licensed by the MAS will be caught. These smaller agents may deal with customers and record confidential

S/N	Respondent	Feedback from respondent
		information during the sales process on their devices. To this end, we seek clarification on whether the Notice is intended to also be applied to these agents who distribute insurance products. A participant suggested that MAS considers an approach of putting FIs into different buckets and applying different cyber hygiene practice requirements. For example, implementing a Security Standard for an entity with very few staff (e.g. 1 or 2) may not be a necessary requirement. **2. Comments on the proposed definitions:** We note that some proposed definitions are consistent with similar definitions in the existing Technology Risk Management Notice. However, some participants highlighted that the definition of ‘system’ may be inconsistent, unclear and may be too broad. The definition of ‘system’ in the existing TRM Notice states that system means any hardware, software, network, or other IT component which is part of an IT “infrastructure”. On the other hand, the definition in the proposed Notice on Cyber Hygiene states that system means any hardware, software, network, or “other IT component” used by the relevant entity. To this end, we would like to suggest that MAS lists out the components that would constitute a system in the Annex of the cyber hygiene practices, for clarity. Participants are concerned that the proposed definition of confidential information is very broad, covering even any information relating or belonging to the relevant entity that is not publicly available. However, it is clear that not all publicly unavailable information would be confidential. This issue is further discussed below, under Question 3 on the multi-factor authentication (“MFA”) requirement. The proposed definition of administrative account of one with full privileges and unrestricted access, seems to suggest that such an account is a super administrative account. We would like to seek MAS’ clarification on whether this is the correct interpretation, and to confirm that the related hygiene practice requirement applies only to super administrative accounts. Some participants highlighted the importance of harmonising the definitions with those used by international standards. Our roundtable noted that the Financial Stability Board had recently in July 2018 issued a consultative document, Cyber Lexicon, and responses and comments have been submitted on 20 August

S/N	Respondent	Feedback from respondent
		2018. The FSB is expected to finalise the Cyber Lexicon by November this year. The Cyber Lexicon is intended to work on the common understanding of relevant cyber security and cyber resilience terminology and practices. While it is still in the consultation phase, we seek MAS' consideration to finalise the Notice in tandem with the international standards as differences in definitions may have implications on intra-group outsourcing arrangements. **3. Comments on the proposed cyber security requirements:** Participants at the roundtable were generally of the view that the Notice covers all the fundamentals of cyber security practices. Regarding the requirement for administrative account to have strong password controls, participants would like to seek MAS' clarification on whether implementing password manager would be an acceptable practice. Some participants were of the view that the requirements on security standards proposed by MAS seem ambiguous. While we understand that the measures may vary according to the differences in the scale, complexity and nature of the relevant entities, having security standards can be challenging to fintech firms and very small entities, including sole proprietors such as money changers. Participants would also like to know if MAS would be providing a list of acceptable international security standards that relevant entities can use. Regarding the guidance on implementing one or more firewalls at the network perimeter in order to segment the internal network from the public internet., we seek MAS' clarification on whether it is expecting relevant entities to implement internet surfing separation, such that laptops used for ther internal network and systems cannot be used to access the public internet. While MAS states that MFA is one of the cyber hygiene requirements, it is unclear whether the second or more factor can be of the same vector. For example, can the first factor be ID and password, and the second factor also be password-based (or PIN). We seek MAS' clarification whether MFA requires different vectors. Participants also noted that in the definition on MFA, examples of factors given did not include SMS. The industry typically

S/N	Respondent	Feedback from respondent
		issues SMS as a second factor and we would like to suggest that MAS lists this as an example. Participants are also concerned that the proposed requirement to have MFA on all accounts with access to confidential information through the internet will result in a need to implement MFA for many accounts, including the unintended. This is because the proposed definition of confidential information is very broad, covering even any information relating or belonging to the relevant entity that is not publicly available. There are in fact much information about the entity itself that are not publicly available but are clearly also not considered confidential. We suggest that MAS considers tightening the definition of confidential information and not inadvertently require that MFA be implemented on the accounts that it had not intended. Training is crucial to spotting and reporting cyber incidents in a timely manner. While MAS may not have intention to make training a legally binding requirement, MAS may wish to consider issuing it as a guidance, for example, in its proposed cyber hygiene practices in the Annex. **4. Comments on the proposed transition period:** Participants were concerned that the implementation of MFA would be challenging given that many of them would need time to source for solution providers at the same time. Relevant entities would require a substantial time period to enhance their existing IT policies, procedures and standards, and make necessary amendments, where applicable, given that the Notice would also affect its outsourcing arrangements (intra-group or with third party service providers). Some participants find that the 12-month transition period may not be feasible for relevant entities to implement all of the expected cyber hygiene practices at one time given the varying degrees of complexities of the practices such as setting up the relevant framework or tweaking the existing standards and practices, implementing enhanced tools such as MFA and sourcing for the availability of technology to comply with the Notice. To this end, some respondents would like MAS to consider a staggered timeline given for the implementation of different practices, with more time given to the MFA requirement.

S/N	Respondent	Feedback from respondent
		As some FIs may have more resources than others, and in consideration that some classes of FIs are smaller, participants would like MAS to consider bucketing entities, and giving small FIs a longer timeline to comply with the Notice. **5. General Comments:** RHT Compliance Solutions conducted a roundtable discussion with industry members/financial institutions on the proposed cyber hygiene practices requirements in the Consultation Paper. The roundtable was attended by 64 attendees from 53 companies on 27 September 2018. Participants comprised representatives from banking and capital market industries, including locally incorporated banks and Singapore branch of foreign banks, payment service providers, Fintech companies and other financial institutions. We share the view that it is critical to have good cyber hygiene practices and are supportive of the proposals. However, we request that MAS considers the implications of some of the practices proposed in the Notice on Cyber Hygiene (the “Notice”). Our comments on the questions posed in the Notice are set out below and incorporate, where appropriate, inputs received from the roundtable participants.
79.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** The term “significant disruption” is used under “critical system” yet I do not see a definition for this. To avoid ambiguity, I suggest that this be defined and not left to the discretion of the individual institutions given they serve such a critical part in the community. There is an increasing tendency for some institutions towards the use of open source software. Given the potential vulnerabilities, the term “software” as used in the definition for “systems” such explicitly include any such open source software. Under the term “vulnerability”, the term refers to “unauthorised person”. As system vulnerabilities can also be compromised by insiders, this definition should include malicious acts by employees who may hold the relevant authorisation. **3. Comments on the proposed cyber security requirements:**

S/N	Respondent	Feedback from respondent
		The written security standards must be approved by the institution's senior management including the relevant CEO and CRO (or other suitable person e.g. Compliance). As reported in Channel NewsAsia, the chief executive of the Cyber Security Agency of Singapore, Mr David Koh, said that CEOs and other decision makers must be held accountable whenever a cybersecurity breach takes place. The written standards must include any work undertaken by either that institution's overseas office or any external/managed service provider. In this manner, the integrity of that institution's Singapore infrastructure and its attendant data are given the right attention by stakeholders who must be held personally accountable for any shortcomings, inadequacies, lapses or breaches. Note that breaches arising from an overseas office or external service provider impacts customers of a Singapore linked institution thereby negatively affects the name and reputation of Singapore as a Global Financial Centre. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** 1. Given the criticality of cyber security, the use of the term "hygiene" may unintentionally downplay the importance of the basics. On the note, I suggest that this measure be reworded as "Cyber Duties and Obligations" to give it the appropriate emphasis. 2. In the interim report from the Australian Royal Commission into Banking, Superannuation and Financial Services, there was an entire section on "Processing Errors". A Financial Institution (FI) which is not able to support its services with the required standard of care and in accordance with contractual terms ventures into the area of misconduct as it would have failed to discharge its obligations in a fair and acceptable manner. This needs to be emphasised so that management and staff of the FI give this the proper standard of care. These are not merely "technical errors" and represent a failure of management to set and enforce the required standards.
80.	Aon Singapore Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:**

S/N	Respondent	Feedback from respondent
	Aon Benfield Asia Pte Ltd Aon Hewitt Wealth Management Pte Ltd Aon Singapore (Broking Centre) Pte Ltd	No comments. **3. Comments on the proposed cyber security requirements:** Aon's Comments: Paragraph 5(b) requires a relevant entity to institute controls to reduce risks where there is no available security patch. However, in certain instances where the system vulnerability discovered can only be addressed by way of patching (and unavailable at that point in time), there may not be alternative controls to prevent attackers from exploiting the vulnerability. Can MAS clarify what type of controls would be considered acceptable in such instances? Will a risk assessment of the vulnerability by the FI suffice? Paragraph 9(b) requires a relevant entity to implement multi-factor authentication ("MFA") for all accounts on any system used by the relevant entity to access confidential information through the internet. We note that the MAS TRM Guidelines recommends FIs to implement two-factor authentication for their online financial systems, and there is no similar guidance in the MAS Outsourcing Guidelines. Can MAS clarify if the MFA requirement would apply to information systems hosted by third-party service providers and which contain confidential information? If it does apply, it may not be possible for FIs to impose the MFA requirement on systems hosted by their existing third-party service providers which do not have such MFA capability. Appreciate if MAS could reconsider this requirement for third party-providers or provide alternative options in relation to this. **4. Comments on the proposed transition period:** Aon's Comments: We would like to request a longer transition period of 2 years or more to comply with the MFA requirement. There are existing systems which will require MFA controls to be put in place, and as some of these systems are procured and used on a global basis, more time will be required to coordinate with global stakeholders and negotiate with third-party service providers in implementing the MFA controls. **5. General Comments:** No comments.
81.	Anonymous	**1. Comments on the applicability of the Notice:** No comments.

S/N	Respondent	Feedback from respondent
		2. Comments on the proposed definitions: "administrative account": We will like to clarify on whether the concept of administrator extends to bank's customers who manage their users (access, bank rights) within their organization. "multi-factor authentication" : 1. We will like to clarify on whether client authentication software with token on the same machine can be considered as two-factor authentication. 2. We will like to clarify on whether secured access on a restricted area/room and access to a machine with password can be considered as two- factor authentication. 3. We will like to clarify on whether client authentication software (verified at our site) and a secured physical access to machine (at client's site) can be considered as two- factor authentication. **3. Comments on the proposed cyber security requirements:** "Multi-factor Authentication": We will like to clarify on whether multi-factor authentication is required for any user login (i.e. user without sensitive services)? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** We will like to clarify on whether the proposed Notice covers only local subscriptions from local access or access to Singapore account data from an access point located in another country.
82.	Anonymous	**1. Comments on the applicability of the Notice:** • The scope covers all MAS licensed, approved, registered or regulated entities (each a "relevant entity"); however, some risks imposed on relevant entities may stem from third- and fourth-parties with whom they collaborate. While MAS may not regulate those external parties, it might still consider imposing responsibilities on the regulated entities to ensure good hygiene practices from these external parties • MAS may consider introducing tiered applicability of the hygiene practices, based on regulated entity significance or criticality **2. Comments on the proposed definitions:** a) "Administrative account". Overall, we agree that "Administrative account" must be flagged out for enhanced

S/N	Respondent	Feedback from respondent
		cyber hygiene. However, there are additional considerations and factors relating to other types of accounts. • We suggest defining different level of privilege access or risk-tiering of accounts based on: - The required intensity of administrative rights and the platform in use - Whether Administrative accounts have privilege rights - User access privileges to systems that provide access to non-public information - A defined periodical review of the access privileges • We further suggest distinguishing Elevated accounts from all Administrative accounts: - Elevated accounts are equally 'powerful' accounts, despite not having full privileges to a system. In addition, they pose security risks to an organization, if not secured properly - Recommend using the term "Privileged account" and defining it accordingly b) "Confidential information". • We suggest clearer definition to "Non-publicly available information", aligning with those in existing legislation or regulations (such as PDPA and the GDPR). For example, any information, in its electronic and non-electronic form, relating to: - Personal particulars (for example personal identifiable information) of all customers of the relevant entity, that is not publicly available; complying also with PDPA and GDPR - Business-related information concerning or belonging to the relevant entity that is tampered with, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the institution - Information or data, except age or gender, of an individual in any form or medium created by or derived from a health care provider • We looked at comparable regulatory documents from other jurisdictions and suggest to further consider the reverse definition of "Publicly available information": - Any information that an institution has a reasonable basis to believe is lawfully made available to the general public; provided there is reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine c) "Critical system".

S/N	Respondent	Feedback from respondent
		• We suggest the definition of "system" to be more harmonized across existing regulations to avoid variation of judgement • We suggest "system" to be defined more accurately as "Information System". An example definition: - "A discrete set of electronic information resources organized for all the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems" • We believe that being "Internet-facing" should be another criterion and would suggest including additional criterion for criticality: "Any system that is internet-facing" d) "Multi-factor authentication (MFA)" • Based on the Notice description, we believe that remote access is also included as part of required MFA implementation, though not clearly included. Therefore, we suggest including "remote access" in the definition, as part of implementation of MFA **3. Comments on the proposed cyber security requirements:** Para 4) "Administrative account". • We suggest adding a statement on acceptable compensating controls in lieu of MFA for Administrative or other Privilege account user IDs for organizations with legacy systems that cannot support MFA due to technical limitations. For example: - Compensating controls may include, but not limited to, implementation of dual control for passwords with auditing capabilities using password vault managers which are governed by the organization's change management procedures, or setting up dedicated, isolated machines for all administrative tasks to critical systems with disabled remote access - Implementation of local certificate authentication • We further suggest adding a requirement on incident management, specifically on alerting when administrative groups are modified. For example: - Configuring alerts for accounts added to the domain administrator groups, or deploying automated logging tools like Security Information and Event Management systems • We also suggest including active risk mitigation in finding and eliminating dormant administrative accounts (no access for more than a stipulated period as defined by the regulated entities)

S/N	Respondent	Feedback from respondent
		Para 6) "Security Standards". Overall, the clause under this sub-section ought to be more comprehensive to be relevant. • In general, security standards are recommended to address and highlight the following areas of key concerns: - Setting security standards that include identification and prioritisation of systems and assets. This should vary by criticality, and hence differing standards of the information systems - As part of "deviations from the security standards", the process should consider active review of approved deviations annually (or other frequency as determined by the relevant entity) to validate the deviation and evaluate the systems and their conformity to standards - Ensure all security standards are reviewed and updated when needed, on a reasonable and regular basis, as determined by the relevant entity • We suggest the following items to be considered as additional hygiene practices to the proposed security standards: - Establish a robust and effective communications plan to convey any changes made to the standards (when necessary) to all direct parties concerned - Establish an incident response plan to document and exercise response procedures and plans, including a clear delineation of roles and responsibilities within the regulated entities: ▪ Internal: To senior management and the Board (providing direct reporting line from IT analysts through to CEO office) ▪ External: To authorities and regulators (reporting framework for significant cyber incidents designed to collect and store information on cyber incidents; information to be used by regulators and agencies and monitors trends to understand and contain the exposure ▪ External: To forensic investors and threat management vendors (to address, contain and mitigate cyber threat) ▪ External: To notify affected customers/ clients in the event of data breach (based on existing regulations i.e. PDPA, GDPR) • We further suggest conducting regular cybersecurity education and awareness trainings: - Personnel and partners should be provided ongoing cybersecurity awareness activities to be adequately trained to perform their information security-related duties and

S/N	Respondent	Feedback from respondent
		responsibilities. Such trainings should have metrics with tracking and auditing capabilities, for example, through enterprise learning management systems Para 7) "Firewall" • As part of the "regular review", we suggest active measures to be taken for review and implementation of firewall rules that have not been used by any system for a defined period Para 8) "Anti-virus". • We suggest prescribing the following elementary good practices, for example: - Regular review of individual machines "anti-virus" protection status, including those that have not been connected to the network - Use of automated tools to actively monitor and update software and signatures - All detection events across network servers, workstations, corporate mobile devices, including all other endpoint devices, should be sent to enterprise and event log servers for analysis Para 9) "Multi-factor authentication". • We suggest additional considerations: - Where MFA is not deployable, alternative compensating controls, such as having the accounts on dual-control or split knowledge, should be adapted - Where MFA cannot be implemented due to system constraints (such as legacy banking systems not supporting MFA), compensating controls should be implemented in lieu of MFA - MFA implementation should be the end goal and there must be a committed timeline for migration of such legacy system or change implementation to support MFA **4. Comments on the proposed transition period:** • The proposed 12-month transition period for compliance is a realistic timeframe as most of the requirements set forth should already exist in most relevant entities, though potentially implemented differently • We suggest a dispensation model, whereby relevant entities need to report any inability to comply within a stipulated duration within the 12-month transition period, including a clear work plan and a counter-proposal timeline to achieve full compliance

S/N	Respondent	Feedback from respondent
		5. General Comments: Overall, we recommend MAS to propose guidelines and hygiene practices that are both prescriptive and risk-based. We also strongly suggest the Notice to adopt a more succinct language, with definitive and technically feasible requirements. The additional considerations are highlighted below: • Determine risks and scope by evaluating factors such as critical business functions and importance of the activities relative to the overall market • As part of implementing the cyber hygiene practices over the proposed 12-month transition period, and/or as part of devising a dispensation model over counter-proposed timeline, we suggest MAS to formalize the reporting of gap analysis: Relevant Entities should (1) evaluate where they stand at the beginning of the rollout, including assessing risks of the relevant entity's information systems, (2) submit a clear plan on how they plan to plug the gaps, and (3) the timeline of fulfilling the requirements • Harmonize the Financial Services sector's critical designation with existing definitions, terms and criteria • Require confirmation (and approved documentation) on all proposed standards by defining accountability and associated governance/ oversight, review, control, metrics/ monitoring, or quality assurance arrangements associated with the sustained fulfilment of the cyber hygiene practices. Furthermore, ensure consistency with the MAS proposed guidelines on Individual Accountability and Conduct • Evaluate MAS' expectations and applicability of regulations on critical information systems, including third- and fourth- parties' systems, for example: consider the potential systemic risks associated with large vendors such as public cloud providers • Ensure consistency with pre-existing and related regulations such as Cybersecurity Act (Feb 2018) and Personal Data Protection Act (revised July 2017) and harmonize fragmented regulation to reduce the risk of conflicting/ confusing standards and inefficient compliance costs
83.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** 1. Current definition of "administrative account" may restraint the type of administrative account that malicious hacker(s) is/are of very much interested in, while MAS intends to ask FIs to safeguard it.

S/N	Respondent	Feedback from respondent
		Depending on systems application design, and its access control matrix, standalone "administrative account" may or may not have "Full privileges" and many of the critical application may only give out "restricted" access right to a standalone administrative account. 2. MAS defines "confidential information" as any information that "is not publicly available"; According to international practices in running an information security management system, information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure, while legal requirement is one of the factors. Except for the factor: legal requirement, the definition of confidential information, shall normally come from an entity level data risk assessment process; If MAS, as a regulatory body, gives out a clear legal definition to FIs on this term, it may restrain the possible ways for business entity classifying their data asset when handling their data risk, thus this proposed definitions to be used may then deem as unsuitable. Reference: ISO_IEC_27002:2013 section 8.2.1 Classification of Information, control statement: " Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification." While implementation code of practice stated that "Classification should be included in the organization's processes, and be consistent and coherent across the organization." **3. Comments on the proposed cyber security requirements:** 1. Para 4- Cyber Hygiene Practices: Administrative Accounts "A relevant entity must secure every administrative account on its system to prevent any unauthorised access to or use of, such account" The coverage of this proposed requirement on this para 4 may suggest a non-exhaustive list of systems used by FIs. It may be

S/N	Respondent	Feedback from respondent
		inefficacy to apply the same level of security controls and safeguards to every system, while in fact the criticality of systems varies. We ask MAS to consider limiting the scope to Critical system only. 2. Para 6- Cyber Hygiene Practices: Security Standards The proposed requirement stated in Sub-paragraphs (6b) and (6c), would imply a regular assessment/review of entity's systems compliance or to their defined security standards. We would like to seek MAS's consensus to allow the firm to have autonomy in defining our own security assessment review frequency, in accordance with the firm's risk appetite or risk handling approach. This will enable the firm to invest the resources on top key risk based on cyber intelligence reports. 3. Para 9- Cyber Hygiene Practices: Multi-factor Authentication Considering the current definition of "confidential information", the proposed requirement stated in sub-paragraphs (9b), would have great implication to all web-based and online accessible system to implement 2FA, regardless of the system criticality and system functionality. Thus, we would like MAS to: (A) reconsider the current definition of "confidential information" described in Section "Definition"; (B) To enhance clarity on the compliance with this cyber hygiene requirement: i. if the firm does not provide any online financial / payment services through the internet, it is understood that the multi-factor authentications requirement is not applicable for systems in this definition? Note that there is a security measure in place having the multi-factor authentication mechanism when employees access systems from outside of the office through the internet. ii. Consider limited the scope of sub-paragraphs (9b) to FI's critical system; iii. consider modifying the example given in 2nd bullet points of respective Para 9, under section Annex B, to say "an account belonging to Human Resource Department that can be used to remotely access staff information through the internet using company remote access mechanism. **4. Comments on the proposed transition period:**

S/N	Respondent	Feedback from respondent
		No comments. **5. General Comments:** No comments.
84.	Anonymous	Confidential
85.	Anonymous	Confidential
86.	CyberArk Software (Singapore) Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** "administrative account", in relation to a system, means any account that has privileges and unrestricted access to the system; Here are some common types of privilege accounts: <u>Domain Admin Account</u> These accounts are typically non-personal accounts and have the full privilege access across all the workstations and servers on a windows domain. While these accounts are few in number, they provide the most extensive and robust access across the network. With complete control over all domain controllers and the ability to modify the membership of every administrative account within the domain, a compromise of these credentials is often a worst case scenario for any organization <u>Local Admin Account</u> These accounts are typically non-personal accounts and provide administrative access to the local system. These accounts are typically used by IT staff to perform maintenance on workstations, servers, network devices, databases, mainframes etc. Often, they share the same password across an entire platform or organization for ease of use. Such sharing of password across thousands of hosts makes it an easy soft target that advanced threats routinely exploit. <u>Privilege User Account</u> These are typical named user accounts granted with administrative privilege(s) to one or more systems within the network. This is typically one of the most common forms of privileged account access granted on an enterprise network, allowing users to have administrative rights on, for example, their local desktops or across the system they manage. The power they wield across the managed systems make it necessary to continuously monitor their usage.

S/N	Respondent	Feedback from respondent
		Service Account These accounts are non-personal accounts, local or domain accounts that are used by an application or service to interact with the operating system or network. In some cases, these service accounts have domain administrative privileges depending on the requirement of the application they are being used for. Local service accounts can interact with a variety of Windows components which makes coordinating password changes difficult. Application Account These accounts are accounts used by application to access databases, run batch jobs or scripts or provide access to other applications. These privileged accounts usually have broad access to underlying company information that resides in applications and databases. Passwords for these accounts are often embedded and stored in unencrypted text files, a vulnerability that is replicated across multiple servers to provide greater fault tolerance for applications. This vulnerability represents a significant risk to organization because the application often host the exact data that APTs are targeting. Studies have shown that to facilitate the uptime of the applications, these applications accounts are usually not managed and rotated. Organizations have indicated and accepted this as a risk. This results in a unmanned backdoor into the organization and often straight to the crown jewels such as the database or domain controller. Emergency Account Sometimes referred to “break glass” or “firecall” account, these accounts are assigned with local or domain administrative rights to secure systems in case of an emergency. While access to these accounts typically requires a managerial approval for security reasons, it is usually a manual process that is inefficient and lacks any auditability. **3. Comments on the proposed cyber security requirements:** Administrative Accounts: A relevant entity must secure every administrative account on its system to prevent any unauthorized access to or use of, such account. (a) Access to privilege accounts should be managed by a privilege account security system a. User access to server to perform administrative task

S/N	Respondent	Feedback from respondent
		b. Application and Scripts access to server/application such as database c. Application/Service containers in a DevOps pipeline to access server/application such as database and/or other application (b) All privilege accounts should have its password and/or SSH key pairs rotated randomly by the privilege account security system to prevent any unauthorized usage of these account (c) An unmanaged or new privilege account should be able to be detected by the privilege account security system a. The identified privilege account could be configured to be auto enrolled under the management of the privilege account security system b. The identified privilege account credential should be automatically rotated to prevent unauthorized usage of the account(s) (d) All privilege account usage should be tracked with full audit trail such as username, account name, date, time, source IP, destination IP and activities (e) The privilege account could be enforced with workflow such as 2nd level approval before the access could be granted (f) The usage of the privilege account(s) should be tracked and analysis for any potential bypass of the privilege account security system (g) The privilege account activities should be monitored for mis-use and provide near real-time intervention when needed. (h) Privilege service account should be monitored for unusual activities such as interactive logon **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
87.	Anonymous	Confidential
88.	Anonymous	Confidential
89.	Tokio Marine Life Insurance Singapore Ltd.	**1. Comments on the applicability of the Notice:** Tokio Marine Life Insurance Singapore (TMLS) would like to seek clarity on whether the Notice extends to tied agents as well. This is because tied agents are independent parties and the insurer may only have limited control over their use of IT components, such as mobile devices (e.g. phones, laptops). Should an agent or agency team breach the requirements, would the insurer be accountable too?

S/N	Respondent	Feedback from respondent
		Also, is the proposed Notice intended to cover the practices of third parties (both outsourcing and non-outsourcing arrangements) used by the insurer? If so, a 12 months transition period may not be sufficient. **2. Comments on the proposed definitions:** TMLS wishes to clarify on the following: • Confidential information: To avoid any ambiguity and to facilitate consistency within the industry, it may be better to give more clarity on what would constitute as "publicly available" information. For example, the organization chart of the organization is often not publicly available, but it is typically not regarded as confidential information either. Also, in the event business confidential is leaked by an unauthorized person, once it goes into the public domain, does it imply it is "publicly available"? • Critical System: The definition of "critical system" in the CP is largely similar to the one in MAS Notice 127. TMLS would like to clarify if the 2 terms are referring to the same kind of system? It would be in the interest of all that there is a consistency between the 2 Notices, or if the intention in the Notice on Cyber Hygiene, to be clearer which types of systems are in scope. • Multi-factor authentication: The three characteristics (i.e. what you know, has and is) provides a set of useful principles to identify multi-factor authentication. However, for (b) "something the account holder has" seems to make refer more to a hardware device. TMLS would like to clarify if OTP received via SMS or email address would fall into this category of acceptable multi-factor authentication. For example, based on our understanding, SingPass currently uses email to send OTP for "forget password" function. TMLS also wishes to understand the provision of multi-factor authentication to accessing all our servers and devices that are hosted on the cloud. • System: The term defined is too wide and extensive, and there needs to be a boundary or parameters that MAS needs to come out with as to what is the minimum standards for protection to "Systems" as systems can refer to application, operating system, firmware, Wifi & network device, laptops/desktops, terminals, kiosk, POS, MFD, printers etc. **3. Comments on the proposed cyber security requirements:** TMLS would like to clarify on the following: • Administrative Accounts:

S/N	Respondent	Feedback from respondent
		o What is the scope of responsibilities regarding administrative accounts? Does it span to laptops/desktops, application development, routers, etc? • Security patches: o TMLS would like MAS to clarify on the components that it feels FI(s) should be focusing on to include into the framework. Patching can cover a very broad spectrum of software/hardware components and as such TMLS request clarification if there should be a list of key components that FI(s) should prioritize over others for patching as these components are the most critical e.g. OS, database, etc. o TMLS agrees that FIs should institute controls to reduce the risks posed by vulnerabilities in the system. However, there would be instances where a solution may not be available for any risk reduction. For such instances, TMLS would suggest that FI have the ability to accept the short-term risk if it is within the risk tolerance of the company, while waiting for the security patch to be made available. In addition, TMLS would suggest to reword the statement "… any risk posed by such vulnerability…" to "...any known risk posed by such vulnerability..." to better scope the requirements and intent of this clause. • Anti-virus: o As viruses are a subset of malware, TMLS would like to propose for the term "Anti-virus" to be reworded to "Anti-Malware" in order to be more consistent and encompassing. • Multi-factor Authentication: o Understand that it is a common practice among FI(s) to only trigger the use of multi-factor authentication when the user is carrying out "higher risk" transactions. For example, logging into an online portal normally only requires the use of userid and password. This enables the user to have limited view and functionality in his own account. Only when the user needs to carry out certain "higher risk" transactions or view more detailed information that a 2FA is triggered. TMLS would like to seek MAS' clarification on need for multi-factor authentication at both the login stage and the transaction signing stage? **4. Comments on the proposed transition period:** TMLS opines that the notice will realistically require 18 to 24 months to be implemented, given the requirements to implement security standards to all the systems within the FI and the possibility to ensure similar standards are being impose to our service providers.

S/N	Respondent	Feedback from respondent
		5. General Comments: The 6 hygiene factors introduced is a good start for FIs to strengthen their cyber resilience. Below are a set of cyber hygiene baseline practices* introduced by Carnegie Mellon University that MAS may take into consideration to make the Notice more comprehensive. (Source:https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf) 1. Identify and prioritize key organizational services, products and their supporting assets. 2. Identify, prioritize, and respond to risks to the organization's key services and products. 3. Establish an incident response plan. 4. Conduct cybersecurity education and awareness activities. 5. Establish network security and monitoring. 6. Control access based on least privilege and maintain the user access accounts. 7. Manage technology changes and use standardized secure configurations. 8. Implement controls to protect and recover data. 9. Prevent and monitor malware exposures. 10. Manage cyber risks associated with suppliers and external dependencies. 11. Perform cyber threat and vulnerability monitoring and remediation. In addition to the baseline practices by Carnegie Mellon University mentioned above, TMLS would also like to propose encryption of confidential data to be one of the cyber hygiene practices. In our opinion, encryption is an important aspect in minimizing cyber security risks as it prevents the intruder from reading the data even though he may have gained procession over them. It should be noted that some practices may be too costly for certain FIs to implement. TMLS would like to suggest for such cases, FIs should have the ability to conduct a risk assessment on the associated risk, and have the discretion of not implementing the practice, and put in controls to lower the risk pose by such non-conformity instead. In other words, 6(c) should be applicable to all the hygiene practices and not limited to Security Standards.

S/N	Respondent	Feedback from respondent
		TMLS would like to seek clarifications from MAS if it is mandatory to also impose these hygiene practices on the outsourcing and non-outsourcing service providers engaged by the FI. The measures mentioned in Annex B is a good starting point to guide FIs to comply with the cyber hygiene requirements. TMLS would appreciate it if MAS can provide more examples or guidance of the measures to be provided. Comments on potential addition to the Cyber Hygiene Practices • Centralised Logging and Activity Monitoring: o We have observed that logging and monitoring is not part of the 6 Cyber Hygiene practices. As observed from the recent SingHealth incident, where the DBA during his/her routine maintenance realised an anomaly, an effective monitoring system would have been able to pick up this activity and would have provided a last line of defence. TMLS would like to ask what is MAS' stand on centralized logging and monitoring.
90.	Anonymous	Confidential
91.	Lombard International Singapore Pte. Ltd.	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** "administrative account": • Make the distinction between privileged accounts and administrative accounts • Privileged accounts should be formally included as they could have elevated access rights without being full administrators; Whenever possible, the definitions should take into account existing, internationally recognised, frameworks like ISO 27000, ISO 27001 and COBIT. **3. Comments on the proposed cyber security requirements:** Administrative accounts; • Should implement detective controls (session recording and monitoring, log review) for administrator's operations; Security patch: • Should define a vulnerability management framework to regularly test the systems for potential weaknesses and missing security patches;

S/N	Respondent	Feedback from respondent
		• Should define a system lifecycle policy and ensure that IT assets are updated / replaced in line with the technological progress (to avoid unsupported assets from being used in production environment). Security standards: • Should use, whenever possible, internationally recognised security standards that are relevant to your organisation (to avoid the definition of security standards that are not, in fact, secure). Firewall: • Should deploy firewalls to segregate internal zones with different security levels; • Should isolate the core networking (servers, appliances etc.) from the end-users' network. Only allow the required traffic to be exchanged between the different security zones. • Should disable completely the remote management of perimeter firewalls or allow it only from specific IP addresses. Antivirus: • Should deploy antivirus solutions relevant to the system and operating system in use, the purpose of the system and the interaction with other systems; • Should take into account that many antivirus solutions are not 100% effective and consider the deployment of other antimalware solutions (host based or network based) to detect or prevent malicious behaviour. Multi-factor authentication: • Should implement multi-factor authentication for any remote access sessions whether they are for remote application access or for technical support purposes; • Should consider the risk of denial of service associated with multi-factor authentication mechanisms directly accessed via the Internet, especially those based on one time passwords; Should implement information security function: See http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf16_647eng.pdf The Information Security Officer (ISO) shall be the person in charge of the organisation and management of the information security, i.e. the protection of the information. S/he shall be

S/N	Respondent	Feedback from respondent
		independent from the operational functions and, depending on his/her position and the size of the undertaking, released from the operational implementation of security actions. An escalation mechanism shall enable her/him to report any exceptional problem to the highest level of the hierarchy, including the board of directors. His/her key missions are the management of the analysis of the risks related to information, the definition of the required organisational, technical, legal and human resources, the monitoring of their implementation and effectiveness as well as the development of the action plan(s) aimed to improve the risk coverage. Should implement information security policies and procedures: • Define information security policies and procedures, perform regular reviews and ensure that they are communicated to all staff and relevant third parties Should implement information security awareness: • Organise regular campaigns to improve the awareness level among staff; • Perform regular phishing or social engineering exercises to test the staff's awareness Should implement web application security: • All internet facing web applications shall be tested regularly from security point of view (pentest); • Information security requirements shall be embedded during the development stage of the web application; • Input validation controls shall be implemented and tested Should implement information exchange security: • Consider using mandatory TLS whenever possible for e-mails exchanged with relevant third parties; Should implement logging and monitoring: • Solutions for logging and monitoring shall be deployed and their output shall be monitored or reviewed on regular basis; Internet access: • Web proxy solutions shall be deployed to prevent malicious content from connecting to external locations or services (e.g. phishing e-mail trying to connect to malicious website to download payload);

S/N	Respondent	Feedback from respondent
		Additional sources: The list of controls defined in Annex A of ISO 27001; The cybersecurity requirements included in NY DFS 500 regulation https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf **4. Comments on the proposed transition period:** 12 months is ok. An 18 months could also be considered with a progressive enforcement of various sections across the entire period. **5. General Comments:** No comments.
92.	BNP Paribas Singapore Branch	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** <u>Critical system</u> We respectfully request that the Authority provide greater guidance and clarification on the definition of “critical system” for the purpose of this Notice; if the applicability of the definition of “critical system” is similar to that for the MAS Notice 644. <u>Multi-factor authentication</u> We request that the Authority provide more guidance and examples on the types of behaviour that could be considered as a “multi-factor authentication” factor. <u>System</u> We would like to seek clarification from the Authority if the “system” used by the relevant entity is limited to only those maintained in Singapore, or if it involves all systems, including those maintained outside of Singapore but used by a relevant entity in Singapore. **3. Comments on the proposed cyber security requirements:** <u>Administrative account</u> We respectfully request that the Authority provide greater guidance on the following: - If technical accounts used for core infrastructure service falls into this category; - If administrative accounts in relation to daemon falls into the definition.

S/N	Respondent	Feedback from respondent
		This is in view that there are some applications that run interactively and must have privileges, and others require default session interaction without MFA, such as those automated through robots. Anti-virus We respectfully suggest that the Notice requirement to implement anti-virus measures be expanded to include the implementation of anti-malware controls. Multi-factor Authentication We request that the Authority provide greater guidance and specific examples of "accounts on any system used by the relevant entity to access confidential information through the internet". **4. Comments on the proposed transition period:** We respectfully suggest that the Authority take into consideration the complexity of the actions and implementations to be taken on systems to strengthen cyber resilience of FIs as required by the Notice that would result in both local and global impact. Such actions and implementations could possibly exceed the proposed 12 months' timeframe. **5. General Comments:** No comments.
93.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Comment on the proposed definition of 'confidential information': (a) The proposed definition of 'confidential information' includes both customers' information and business information. We are of the view that this definition too wide as the confidential information of the relevant entity that is not publicly available should not be included in the definition as it is part of the risk assessment considerations for that entity. (b) We recommend that similar definitions of 'customer' and 'customer information' that are set out in the MAS GUIDELINES ON OUTSOURCING be adopted instead – the definition of 'confidential information' will only cover customers' information that is limited to customers' information excluding customers' information which is not only public but

S/N	Respondent	Feedback from respondent
		also anonymised, encrypted in a secure manner such that the identities of the customers cannot be readily inferred. **3. Comments on the proposed cyber security requirements:** Comments specifically on Para 9 Multi-factor authentication: (a) We agree that multi-factor authentication for privileged access is the right approach to ensure that the necessary safeguards are in place. However, we are concerned that the proposal under para 9(b) requiring multi-factor authentication to be implemented for all accounts on any system used to access confidential information through the internet. This inclusion will impact all users (not limited to privileged user or access to critical system) as multi-factor authentication will apply to every employee supporting our Singapore office (whether within or outside Singapore) and will need to be put in place once he/ she is working in an offsite location and access is provided via internet. For example, users working from home or away from the office locations require internet access to access the email system or when the Business Continuity Plan is tested or activated. Implementation of para 9(b) will require significant investment. (b) We recommend that para 9(b) be removed from the requirement of Multi-factor authentication as long as we have adopted and implemented physical and logical access security to allow only authorised staff to access our systems and implement the appropriate processing and transmission controls to protect the integrity of our systems and data in accordance with the TRM Guidelines. Alternatively, such multi-factor authentication should only be limited to specific online systems affecting financial and/or transaction-signing for authorising customer transactions and not apply to all types of activity on all accounts used to access the system containing confidential information. **4. Comments on the proposed transition period:** If multi-factor authentication continues to apply to every employee supporting our Singapore office (whether within or outside Singapore), we will need a longer time to budget and implement the requirements. **5. General Comments:** Our observation is that this Notice on Cyber Hygiene, when applied to the financial services industry, may complicate the

S/N	Respondent	Feedback from respondent
		compliance with this Notice and the existing MAS TRM Notice and Guidelines that have been in place since 2013.
94.	Funding Societies Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** We feel that the definition for "Security Standards" is too broad and that it wouldn't be realistic for most organisations to meet. We suggest that this term can be interpreted as global security standards for example NIST framework or the ISO 27001 **3. Comments on the proposed cyber security requirements:** We feel that the Cyber Hygiene Practices for "Security Standards" is very broad and would include all possible controls (including the other 5 practices mentioned). It would be much preferred to remove this item and prioritise the other critical controls We deem insider threat to be a bigger risk and we are suggesting to include DLP (Data Leakage Prevention) as part of the Cyber Hygiene Practices. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
95.	Direct Asia Insurance (Singapore) Pte Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Additional guidance relating to the application of multi-factor authentication to critical system administrative accounts is sought. For example, is it expected that all sub-systems such as network directory services, network devices, etc, require multi-factor authentication? In some cases, multi-factor authentication may not be available on these services. It is suggested that exceptions should be catered for in the same way as security patches and security standards. i.e. the requirement for the organisation to reduce the risk through alternative controls if multi-factor authentication is not practicable. **4. Comments on the proposed transition period:**

S/N	Respondent	Feedback from respondent
		No comments. **5. General Comments:** No comments.
96.	PricewaterhouseCoopers Risk Services Pte. Ltd.	**1. Comments on the applicability of the Notice:** Applicability • The proposed Notice and its applicability to a new category of regulated entities i.e. “licensees under the proposed Payment Services Bill” would introduce legal binding requirements on entities that are currently not regulated. These entities are not currently subject to the requirements in existing Technology Risk Management Guidelines and Notice, hence may not be equipped to comply with the full set of cyber hygiene measures and would need significant effort and resources in order to comply. • The proposed Notice would bind entities regardless of size, so both large and small companies would be subject to the same requirements. Although regulation of these entities is justified on the basis of sensitivity and criticality of data dealt with in the financial sector, certain requirements may be too onerous or costly to implement for small businesses. MAS may consider more specific yet pragmatic minimum standards for all entities including small businesses. **2. Comments on the proposed definitions:** Confidential Information • “Confidential information” defined as “relating or belonging to the relevant entity that is not publicly available” would typically include details of a company’s financial affairs and business operations. The Notice definition may encompass information that is not sensitive in nature but would be deemed ‘confidential’ as the information is not made or intended to be publicly available for example organisation structure, policies and procedures, etc. • The definition in itself is commonly used and applied in both public and private sector. However, there are also various other categories of information classification based on sensitivity of the information to the organisation. The difficulty in applying this definition increases with the requirement to apply multi-factor authentication (“MFA”) to “all accounts on any system used by the relevant entity to access confidential information through the internet”. This requirement does not allow the FI to take a risk-based approach on how they restrict

S/N	Respondent	Feedback from respondent
		and control access to such information that is not publicly available. System • "System" defined as "any hardware, software, network, or other information technology ("IT") component used by the relevant entity" is broad and includes all components regardless of the use and functionality as well as data residing within these systems. For example, ALL databases, operating systems, applications, network equipment, supporting IT components (such as printers, monitors). This definition as it applies to the requirements for 'Administrative Accounts', 'Security Patches' and 'Security Standards' is very broad. Could the MAS provide further guidance to determine the scope of systems to be included as part of the Cyber Hygiene Notice? Multi-factor Authentication • "Multi-factor authentication" means "the use of two or more factors" of "(a) something the the account holder knows", "(b) something the account holder has" and "(c) something that the account holder is". Could the MAS provide further guidance on wether the factors of (a), (b) and (c) must be considered exclusively? i.e Could 2 different passwords for the single account holder be considered 'multi-factor authentication'? **3. Comments on the proposed cyber security requirements:** Security Standards • "A relevant entity must have a written set of security standards for its system". Comments in relation to applying security standards to 'system' as defined in the Notice are provided above in the feedback on definition of 'system' • Further the definition of 'security standards' does not provide guidance on what the standards should contain. Could the MAS provide further guidance on what the security standards should contain? Multi-factor authentication • "A relevant entity must implement multi-factor authentication for…(b) all accounts on any system used by the relevant entity to access confidential information through the internet." Comments in relation to applying MFA to 'confidential information' as defined in the Notice are provided above in the feedback on definition of 'confidential information' Anti-virus implementation

S/N	Respondent	Feedback from respondent
		• “A relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system.” Can MAS clarify if only signature-based anti-virus/anti-malware measures would meet these requirements? **4. Comments on the proposed transition period:** Transition period • The proposed Notice would bind entities regardless of size and maturity of cyber security practices. Therefore certain types of entities may need a longer timeframe than 12 months to comply with the Notice. Most notably the entities that would be included through the proposed “ Payment Services Bill”. Could the MAS give a longer implementation timeframe (more than 12 months) for these newly regulated entities to comply. **5. General Comments:** Third Parties • What is MAS requirement for entities that use third parties in the definition of ‘system’ but where the control over these systems are not within the entities purview? For example, cloud services Overall Feedback • This feedback was based on collective feedback from clients through our dialogue sessions during the consultation period.
97.	Mizuho Bank Ltd., Singapore Branch	1. Comments on the applicability of the Notice: We do not have any substantive comments. 2. Comments on the proposed definitions: We do not have any substantive comments. Comments on the proposed cyber security requirements: We agree with the measures proposed by MAS with regards to the following: Administrative Accounts Security Patch Security Standards Firewall Anti-virus With regards to Multi-factor Authentication (MFA), we do not see any issue with regards to the implementation of MFA for the accounts / services managed by Mizuho. However, we wish to highlight for MAS’ consideration that for accounts / services which are provided by external providers through internet, we may not be able to ensure entirely that multi-factor authentication will be implemented by external providers.

S/N	Respondent	Feedback from respondent
		4. Comments on the proposed transition period: Barring any unforeseen circumstances, the implementation timeline of 12 months from the date of issuance of the Notice seems reasonably feasible. However, we would request a longer timeline for implementation given the number of major system changes / implementations that banks are required to undertake to meet new / revised regulations; e.g. revised MAS Notice 610, removal of ACU-DBU divide, etc. **5. General Comments:** No comments.
98.	Aviva Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** 1) Definition of administrative account should not be limited to user account. It should include non-user accounts such as service accounts and interface accounts. 2) System is defined as any hardware, software, network, or other information technology component used by the relevant entity. Some of these components may not have anti-virus or hardening standards. Are we expected to subject these components to the same requirements/controls as the vulnerabilities may not have relevant patches? **3. Comments on the proposed cyber security requirements:** 1) A relevant entity must secure every administrative account on its system to prevent any unauthorised access to or use of, such account. Please provide guidance on the expected level of security controls for administrative accounts. 2) A relevant entity must implement multi-factor authentication for (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. This requirement may be too onerous for FIs to ensure compliance as confidential information includes any information relating or belonging to the relevant entity that is not publicly available. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.

S/N	Respondent	Feedback from respondent
99.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** We have concerns implementing the current proposal 12 months from the date of issuance of the Notice, specifically the multi-factor authentication requirement. Typical authentication system does not offer default multifactor authentication and it would be difficult to implement on all critical systems as well as all other systems used to access confidential information through internet. Dependencies on third-party systems may further increase the risk in meeting the timeline. **5. General Comments:** No comments.
100.	Investment Management Association of Singapore	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Request to define "customer(s)" in 2: Could MAS define "customer(s) in 2. "confidential information": Confidential information need not necessarily mean information that is not publicly available. The associated risks to relevant entities and business partners (e.g. clients/ vendors/ service providers) should be considered and provided for in the definition. Firms may currently have their own classification scheme, with the definition of confidential information varying across sectors. Many institutions have their own classification scheme. The definition of confidential information varies across sectors. Subparagraph 9b requirement (under Cyber Hygiene Practices section) needs to be explicitly defined and take into consideration that most sophisticated firm has established its data classification system. Firms may use a series of controls to restrict access to sensitive data to specific users or limit it by type. "critical system":

S/N	Respondent	Feedback from respondent
		Members have requested for a more specific definition of "critical system", to possibly include examples which highlight operating criterion (e.g. essentiality, confidentiality, integrity, timeliness and availability) to better guide the implementation. "security standards": Members have noted that there may exist systems i) Which might not have industry security standards or ii) Where security standards are not provided by the relevant vendors. We propose for the MAS to consider amending the current definition to "in relation to a system, means a set of configurations or procedures for the purpose of safeguarding and improving the security of the system". This would provide flexibility to relevant entities in implementing appropriate controls and procedures where security standards are not available. "system": Members have requested for a more explicit definition of "system", given the specific practice requirements on systems (e.g. Multi-factor Authentication, Administrative Accounts). In addition, referring to the portion of the statement "used by the relevant entity", members seek clarification in instances where systems are outsourced, and/or various components are housed or managed externally. In such instances, the entity may not be accessing or using the system to a similar degree as other entities whose systems are kept in-house. **3. Comments on the proposed cyber security requirements:** Administrative Accounts: There needs to be a specific definition for system, in the absence of which could mean a wide scope encompassing the intent that all administrative accounts (e.g. for operating systems, databases, applications, software, network components, and security components) are secured and managed at a heightened policy level. Presumably, the entity can define security policies and adopt a risk-based approach to secure these accounts and ensure the accounts are compliant with these policies. To note there may be some administrative accounts that may not be able to comply with all the policies given the nature of the accounts Additionally, we propose for the MAS to consider amending the current definition to "A relevant entity must take reasonable measures to secure every administrative account on its system

S/N	Respondent	Feedback from respondent
		to prevent any unauthorised access to or use of, such account". Members have feedback that "securing" an account in the technical sense may not be attainable, as one individual at least will have access to an administrative account. Security Patches: We wish to clarify how does Section 5 apply to i) systems outsourced by relevant entities; are systems provided by outsourced vendor but contracted as a "service" (e.g., SaaS, PaaS) covered and; ii) systems that are subcontracted by relevant entities' outsourced service provider (i.e. where relevant entity has no direct contractual relationship)? 5(a) Security Patches: We wish to highlight potential situations where the application of security patches may cause the application to break or render the vendor unable to provide support of the application, which would resultingly impact the relevant entity's operations. Could MAS provide an option in the Notice to allow relevant entities to institute appropriate controls to reduce any risk posed by not applying the security patches to its system where the application of security patches cannot be applied to the system due to system malfunction or invalid vendor warranty support. 5(b) Security Patches: 5(b) should also address situations where patches, even though available, cannot be applied, such as CPU Architectural Design Flaw. Firms may have alternative controls to mitigate the residual risk. Entities may adopt a risk-based approach on their own to secure their accounts by taking a "Comply-or-explain" approach, instead of legislation. Additionally, members wish to clarify the use of "must institute" in the definition, as it may be interpreted to mean mandatory implementation of additional controls to reduce risk, which may be impractical in certain situations. An assessment on sufficiency of existing controls could be considered prior to asking relevant entities to institute controls. Security Standards: We wish to clarify how does Section 6, in general, i) Apply to systems outsourced by relevant entities; are systems provided by outsourced vendor but contracted as a "service" (e.g. SaaS, PaaS) covered;

S/N	Respondent	Feedback from respondent
		ii) Apply to systems that are subcontracted by relevant entities' outsourced service provider (i.e. where relevant entity has no direct contractual relationship); iii) Apply from a standpoint of a Singapore branch of foreign entities; would such entities be able to leverage on existing security standards implemented by their Head Office? 6(a) Security Standards: Can the MAS clarify if a standard suffices for all systems or for a class of system (e.g. servers). The statement is unclear. 6(c) Security Standards: We wish to clarify the use of "must institute" in the definition, as it may be interpreted to mean mandatory implementation of additional controls to reduce risk, which may be impractical in certain situations. An assessment on sufficiency of existing controls could be considered prior to asking relevant entities to institute controls. Firewall: We wish to clarify how would Section 7 be applied/assessed in the context of a global organisation, and if the "network perimeter" pertains only to the Singapore legal entity's network. Anti-virus: Members have highlighted potential situations whereby installing anti-virus (i) would break the application due to performance issues that will impact the relevant entities' operations or (b) is ineffective when installed on Linux/Unix variants operating systems. As such, we kindly request for the Authority to consider the provision of an option in the Notice to allow relevant entities to institute appropriate controls to reduce any risks posed for not implementing anti-virus on the system in situations where anti-virus cannot be implemented on the system as it may result in system malfunction, or non-effectiveness (e.g. Linux, Unix variants of operating system). Multi-factor Authentication: Members have asked if they could still continuously use a critical system if the vendor of that off-the-shelf system cannot implement Multi-factor Authentication and/or for internally-developed systems, for firms relying on existing implementations set forth by their overseas Head Office. 9(a) Multi-factor Authentication:

S/N	Respondent	Feedback from respondent
		The Multi-factor Authentication wording is too broadly worded. Multi-factor authentication should apply to users trying to access the internal network from externally. It therefore makes more sense for retail businesses such as banks (eg. for external access to e-banking) where customers are provided access to systems. Multi factor cannot cover ALL admin accounts and is not feasible for smaller firms. To have a multifactor authentication system in place for internal usage (admin accounts), some sort of IDAM (identify access and management) solution must be in place. These can be costly and resource intensive to implement and maintain. With the vast spectrum of type of institutions in the financial industry which have varying business nature, size, complexity and IT capabilities, we would like to highlight that there might practical challenges faced by relevant entities if this requirement is stipulated as compulsory in the Notice. Thus, we would like to seek the Authority to re-consider whether Multi-factor Authentication requirements should be imposed across all relevant entities or only to certain types of financial institutions. Alternatively, the Authority may wish to consider the provision of option in the Notice to allow relevant entities to institute appropriate controls to reduce any risk posed for not implementing Multi-factor Authentication on applications in situations where the relevant entity has assessed it not to be cost effective or the implementation is too complex, on a risk-based approach. 9(b) Multi-factor Authentication: The wording is too broadly worded. We require more clarity on the requirements and the context to be applied. The statement could be interpreted as relating to i) Virtual Private Network access (i.e. employee login from home office), ii) Customer Login access (e.g. internet banking capabilities), iii) External Vendor Remote Login access (i.e. vendors log into the internet network for maintenance purposes), or iv) External Cloud-based solutions. With different user groups accessing various types of private information, members wish to understand in which instances would the Multi-factor Authentication requirement apply. We also wish to clarify i) How would Section 9 apply to outsourced/externally managed systems;

S/N	Respondent	Feedback from respondent
		ii) Systems that are subcontracted by relevant entities' outsourced service provider (i.e., where relevant entity has no direct contractual relationship; iii) At what level does Section 9 need to be implemented (i.e., whether at OS, databases, applications, software, network components, and security components)? **4. Comments on the proposed transition period:** Members propose for a longer transition period of 24 months, to allow entities sufficient time to assess compliance across systems, remediate any gaps identified and implement any additional technical measures. Members also referenced the transition periods of the General Data Protection Regulation and the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Relevant entities may not have the required technologies such as Multi-factor Authentication in-house and would need to source for the most appropriate product and/or service provider. Additionally, Financial Institutions would need time to engage with their outsourced service providers (e.g. HR payroll vendors, system vendors) who would be impacted by the requirements, in order to work out a feasible resolution. **5. General Comments:** We note that the Notice prescribes cyber security practices which must be implemented. We seek the understanding of the MAS to allow relevant entities the flexibility to institute appropriate controls to mitigate any risk posed in the event that the Notice cannot be applied extra-territorially or on providers who do not fall under the definition of the relevant entities. We also wish to clarify how would the Notice affect affiliated organisations of relevant entities who may be residing in Singapore or elsewhere. Members have also requested for the MAS to consider allowing entities to adopt a risk-based approach in securing their accounts, considering the scope of the definitions provided. We also wish to highlight that no system is entirely impenetrable (e.g. threats such as social engineering may bypass cyber security measures). Members would like to know how the MAS treats non-compliance should members be unable to adhere to certain requirements set forth in the Notice.

S/N	Respondent	Feedback from respondent
101.	Network for Electronic Transfers (Singapore) Pte Ltd	Confidential
102.	Emirates NBD	**1. Comments on the applicability of the Notice:** We do not have any further comments. **2. Comments on the proposed definitions:** With regards to "Definitions" – We suggest to use the term "Critical Asset" rather than "Critical System". We are of the view that "Critical Asset" is a more appropriate term which is applicable to system/applications, hardware devices, people. Please see reference - https://www.techopedia.com/definition/16946/it-asset **3. Comments on the proposed cyber security requirements:** 1) Under Pt 6. Security Standards Quote : 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 – Unquote" Under 6C –Where there is non-conformity, we also suggest the relevant entity to institute a "formal" exception/waiver from their senior management for not conforming to the security standards. 2) Under Pt 7. "Firewall" – Given today's current threat landscape and in relation to cyber hygiene, we suggest to use the umbrella term "Perimeter Defense" to describe security appliances for which the following sub points are featured: - 7a) Network Firewall; - 7b) Web Application Firewall; - 7c) Email Gateway/Filtering; - 7d) Web Proxy; and - 7e) IDS/IPS. 3) Under Pt 8. "Anti-virus" – We suggest to use the term "End Point Protection".

S/N	Respondent	Feedback from respondent
		Antivirus software no longer protects against today's threats, because attacks have become more sophisticated than just virus/malware. Endpoint Protection is a more appropriate term as the tool ensures protection against not just virus/malware but other attacks such as zero-day exploits, advanced persistent threats and inadvertent data leakages. Reference : (1) https://enterprise.comodo.com/security-solutions/endpoint-protection/ (2) https://www.symantec.com/products/endpoint-protection **4. Comments on the proposed transition period:** We suggest that financial institutions be given 24 months from the date of issuance of notice to implement the frameworks, processes and controls to comply with the requirements. **5. General Comments:** No comments.
103.	Anonymous	Confidential
104.	KPMG Services Pte Ltd	**1. Comments on the applicability of the Notice:** Noting that the requirements set in this consultation paper would be legally binding, we foresee that this may introduce challenges to FIs of smaller scale (e.g. money changes, remittance agents, RFMCs). We propose that MAS re-consider the applicability of the notice by adopting a risk-based approach, and potentially roll-out the requirements on a phased approach – e.g. Financial Institutions of higher risk based on the amount of customer information, the size and complexity of their operations. **2. Comments on the proposed definitions:** Confidential Information MAS has defined confidential information as any information which meets both of the following criteria: 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;

S/N	Respondent	Feedback from respondent
		We are of the view that any information which meets any of the above criteria should be considered confidential information. As such, we recommend MAS to update the definition of confidential information accordingly – i.e. replacing 'and' with 'or'. We do not have comments for the definitions for the following: • Administrative accounts • Critical system • Multi-Factor Authentication • Security Patch • Security Standards • System • Vulnerability **3. Comments on the proposed cyber security requirements:** While we understand that the measures suggested in Annex B may not be exhaustive, based on our experience we note that relevant entities may take the regulations by the letter, such that compliance to the Cyber Hygiene Notice is limited to implementing what have been suggested in the Notice. In this regard, with reference to the proposed Cyber Hygiene Practices and the related guidance to comply with the cyber hygiene requirements (Annex B), we note the following: Para 4 – Administrative Accounts • We refer to Annex B where MAS has suggested that relevant entities should "validate on a regular basis that only authorised persons have access to administrative accounts". We understand that while MAS recommends a risk-based approach, we have noted that FIs typically only seeks the minimum acceptable frequency for controls implementation. While we support this risk-based approach, we suggest MAS to provide further guidance, through Annex B, on the acceptable frequency (range) for the validation of access to administrative accounts. • We suggest MAS to add the control requirement/guidance in Annex B – i.e. on maintaining segregation of duties (SoD) in the management of administrative accounts – from the granting, approval, review, monitoring of activities for administrative accounts. Para 5 – Security Patches We suggest MAS to add the following control requirements/guidance in Annex B: • Testing of security patches should be conducted prior to application/implementation to systems.

S/N	Respondent	Feedback from respondent
		• Monitoring mechanisms should be implemented to determine whether patches are applied to systems on a timely manner, such as conducting vulnerability scans, penetration tests, and maintaining a patch inventory. Para 6 – Security Standards No comments. Para 7 – Firewall We suggest MAS to add the following control requirements/guidance in Annex B: • Implementation of at least two (2) or more firewalls, of different brands or models. This is to mitigate the risk of firewalls being compromised from similar security vulnerabilities. • For 'Critical System" or any "system" consisting of confidential information, additional security defence mechanisms should be implemented to complement the existing firewall measures. Examples of security defence mechanisms include (but not limited to): Intrusion Prevention System (IPS) / Intrusion Detection System (IDS) & Distributed Denial of Service (DDoS) / Web Filtering / Web Application Firewall (WAF) protection capability. • Further segmentation of the internal network should be considered to separate the end-user working segment from the segment hosting the IT infrastructure (such as servers, databases, applications). • Segregation of duties (SOD) should be implemented for the management of the firewalls. Para 8 – Anti-virus: We suggest including in Annex B the requirement/guidance to perform periodic monitoring of anti-virus definitions to determine whether the anti-virus definitions are up-to-date and that the anti-virus scans are conducted across all "systems". Procedures should be established to ensure that detected threats detected by the anti-virus scans are responded appropriately. Para 9 – Multi Factor Authentication Based on our experience with the industry, we have noted that most banks have implemented multi-factor authentication on their systems, which should not face challenges as part of this proposed Notice. However, we foresee that other types of FIs will experience challenges in implementing multi-factor authentication on their systems. As such, we recommend the

S/N	Respondent	Feedback from respondent
		consideration of providing alternative measures for secure authentication, such as implementing "never-alone" principle for managing administrative accounts and split-password controls. **4. Comments on the proposed transition period:** We recommend MAS to require/mandate the relevant entities to assess their compliance through a self-assessment within a defined period subsequent to the release of the notice (e.g. 6 months), and full compliance afterwards (e.g. 12 months from the notice release). **5. General Comments:** • Based on our experience with the industry, relevant entities may materially rely on outsourced service providers ("OSPs") on the implementation of these IT controls and proposed Cyber Hygiene Practices (e.g. when management of IT systems are outsourced). As such, we recommend MAS to provide clear guidance on how these practices will be applicable, or to be implemented to the relevant entities' OSPs. While the regulations on Outsourcing requires service providers to comply with Singapore regulations, the linkage between these regulations is not explicit. We recommend for MAS to establish a clear connection between these regulations to provide stronger guidance and direction to the FIs and the outsourced service providers. • We noted that the practices mandated in this notice pertain to preventive or controls to protect the assets of the relevant entities. In order to provide a holistic approach to cyber security, we recommend for MAS to consider including other cyber security controls on detection, response and recovery such as incident management and response (related to the MAS TRM Notice on reporting of relevant incidents), backup management and disaster recovery.
105.	Hannover Rück SE	**1. Comments on the applicability of the Notice:** This notice is easy to read and to understand and well applicable. **2. Comments on the proposed definitions:** With one exception, the proposed definitions are comprehensible and meet best practices. Regarding classification of information, we would recommend to implement at least three classification levels, and that PUBLIC, INTERNAL and CONFIDENTIAL. Currently, this standard includes PUBLIC and CONFIDENTIAL only.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: The proposed six cyber security requirements including their derived measures are clear and plausible. **4. Comments on the proposed transition period:** The proposed transition period is adequate. **5. General Comments:** This notice will help any company to improve its Technology Risk Management System and to reduce its technology and cyber risks.
106.	FWD Singapore Pte. Ltd	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Perhaps, MAS should define the minimum frequency to be reviewed for Firewalls Rules, etc., **4. Comments on the proposed transition period:** 12 months will not be feasible to complete the scope at our end. Consider to give ample time such as 18-24 months for the implementation. **5. General Comments:** No comments.
107.	Legg Mason Asset Management Singapore Pte. Limited	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** <u>Para 9 – MFA</u> o Can MAS clarify to implement MFA for the accounts as stated in the Notice? o Does it refer to all administrative accounts in its system used by the relevant entity (Para 1) or all administrative accounts on its critical system (e.g. an administrative account of an operating system on any critical system), and all accounts on any system used by the FI to access confidential information through the Internet (e.g. an account belonging to the human resource department that can be used to remotely access staff information through the Internet).

S/N	Respondent	Feedback from respondent
		4. Comments on the proposed transition period: No comments. **5. General Comments:** No comments.
108.	Anonymous	Confidential
109.	Singapore Exchange	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Confidential Information – The definition of "confidential information" is too wide and open, and potentially covers a wide array of information including customer comments, feedbacks etc, phone directory etc. Given that FIs are required to implement 2FA to secure such information, this needs to be further tightened. MAS should consider defining "confidential information" by referencing the existing regulations such as SFA/SFR, PDPA etc. Systems – The definition of systems should include technology services. Vulnerability – The proposed definition of vulnerability is incomplete. Example system weakness which could be exploited to deny the use of the systems or compromise the availability or integrity of the system and data. MAS should consider other established references, e.g. FSB drafted Cyber lexicon. **3. Comments on the proposed cyber security requirements:** 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. • Would MAS propose a guideline on what constitute a reasonable timeframe for applying the patches? 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.

S/N	Respondent	Feedback from respondent
		• It will be good if MAS can set out the expectation of the high level technical configuration that should go into the security standard. For example, the CSA Cybersecurity Code of Practice states The security baseline configuration standards shall address the following security principles: a. Least access privilege and separation of duties; b. Enforcement of password complexities and policies; c. Removal of unused accounts; d. Removal of unnecessary services and applications, e.g. removal of compilers and vendor support applications; e. Closure of unused network port; f. Protection against malwares; and g. Timely update of software and security patches that are approved by system vendors. <u>Anti-virus</u>: A relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system. • Given that "system" is defined as any hardware, software, network, or other information technology ("IT") component used by the relevant entity, anti-virus measures are not applicable to some of the components. Hence, we would like to propose "A relevant entity must implement one or more anti-virus measures where available, to mitigate the risk of malware infection on its system." <u>Multi-factor Authentication</u>: A relevant entity must implement multi-factor authentication for the following: (b) all accounts on any system used by the relevant entity to access confidential information through the internet. • We cannot implement MFA on systems we don't own, so we would like to propose "all accounts on its any system used by the relevant entity to access confidential information through the internet." **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
110.	Unicorn Financial Solutions Pte Limited	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: Firewall: If the entity implements virtual desktop infrastructure (VDI) fully, we do not see the need of implementing firewalls for office network. Furthermore, some small entities may work in shared offices like 'Wework workspace', it will not be possible to do so. Multi-factor Authenticatio: Not all systems have multi-factor authentication function. We would like to suggest that if the authentication function allow us to authentic by thumbprint and face recognition, multi-factor authentication is not necessary. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** It is a very common practice to check company emails on mobile phones. MAS should issue cyber hygiene for mobile devices as well.
111.	State Bank of India	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments. **3. Comments on the proposed cyber security requirements:** Reference to the non-exhaustive list of measures set out in Annex B of the Consultation Paper other security controls and processes should also include, Cryptography and Secure Communication : Measures to deter, prevent, detect, and correct security violations that involve the transmission of information. It is essential for disrupting the Cyber Kill Chain. **4. Comments on the proposed transition period:** Transition period is adequate **5. General Comments:** No comments.
112.	Anonymous	**1. Comments on the applicability of the Notice:** Please exclude foreign-incorporated recognised market and recognised clearing houses whose principal regulator is not the MAS.

S/N	Respondent	Feedback from respondent
		2. Comments on the proposed definitions: • The definition of "confidential information": We suggest including concepts which are customarily found in definitions of "confidential information" such as the following: o There should be carve-outs for instances such as a customer having consented to the information being disclosed. o A typical proviso found in other definitions of "confidential information" require that the information is such that a reasonable person would expect that information to be confidential or has actually been indicated to the recipient as being confidential. The relevant entity may be in possession of information which is not publicly available but which would not ordinarily be treated as confidential (e.g. an assessment or report generated by the relevant entity relating to the customer which is not available publicly; this could include a report relating to disciplinary or default management proceedings which is awaiting disclosure to the public by a relevant entity). Further, it is recommended that the undefined "system" term be avoided where possible in favour of a more specific term such as "application," "operating system," "device," or "interface." The frequent use of the undefined term "system" has caused misunderstanding and confusion in implementing regulatory guidance elsewhere when it comes to classifying, inventorying, or assessing the security of "systems". Whether a regulation applies to a server, a set of servers, application code residing on servers, or extends to customers or third-party suppliers are critical factors when implementing controls. **3. Comments on the proposed cyber security requirements:** • Administrative Accounts: Again "system" should be replaced by "operating system, applications, and/or devices". • Security Standards: Again due to widely varying definition of the word "system", we recommend that enforcement of compliance with security standards is applied specifically to operating systems, applications, and/or devices. Further, we suggest that some risk-based limits are placed on this requirement by requiring such standards only where such operating systems, applications and/or devices relate to critical systems. • Firewall: This should be changed to "Network Security" and focus more on the purpose and functionality of network

S/N	Respondent	Feedback from respondent
		security controls that a prescriptive firewall. Specifically the following key controls are recommended in this function: o Network ingress: Firewalls or similar devices should be placed and configured to restrict inbound Internet access to specific approved destinations and services only. Where feasible, sources should further be restricted to networks or locations where customers are known to reside. o Server network egress: Egress from datacenter environments to the Internet should be absolutely limited to only specific destinations and services as required by documented and approved functionality. For example, web servers should not have unlimited outbound to the Internet since compromises frequently abuse that access to establish persistent access, download second-stage malware, and/or exfiltrate data. o Desktop network egress: In office environments, Internet access should be restricted to specific protocols and ports. Further, a web content filtering solution should be deployed and configured to reflect an approved policy of sites and services that are permitted for employee access. o Lateral movement: access control devices should be implemented and configured to segment networks into specific zones such as users, a DMZ, and/or internal database networks. Access control should be configured to prevent lateral access among those networks unless it is explicitly approved and configured. • Anti-virus: This should be renamed to the more current "Malware Protection" title and then can be detailed a bit via the following points: o Endpoints: Devices with inbound or outbound Internet connectivity or those that process files sourced from the Internet should implement anti-malware controls to block malicious content from executing. o E-mail: Inbound mail filtering devices and software should be deployed and configured to block malicious attachments. • Multi-factor authentication: As rightly pointed out under the Annex B, we believe the intention here is to enforce MFA for accounts of an "operating system" on critical systems, therefore we suggest that phrase "operating system" is added under 9(a), so that this section reads as follows: "(a) all administrative accounts on the operating system of its critical system", or similar. Section (b) encounters the challenges noted in section two around the definition of "system". It is recommended this

S/N	Respondent	Feedback from respondent
		is changed to "all accounts on any [application] system used by the relevant… ". More broadly, we suggest that access to data be deemphasised in favour of addressing the risks of destruction, manipulation, or other forms of sabotage; we believe these to be significantly more concerning to critical infrastructure. This should be considered holistically throughout the Paper, but in this specific section it can be reflected via the following addition or similar: "to access confidential information [, control critical systems, or provision entitlements] through the Internet." • [New] Phishing: Educational and technical controls should be designed and deployed to guide employee decision making to avoid malicious social-engineering attacks via e-mail. Content should be provided to help employees detect malicious messages, a reporting mechanism should be defined, technical controls should be deployed to detect known malicious campaigns, and staff should be tested at least annually to measure and reinforce their resiliency to phishing attacks. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
113.	MUFG Bank, Ltd.	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** *(1) "administrative account, in relation to a system, means any user account that has full privileges and unrestricted access to the system"* The term of "unrestricted access" may be open for interpretation. For example, System Administrator would be restricted to OS access without DB access; DBA would be restricted to DB access without OS access. Hence they do not have "unrestricted access". However they should still be considered as "administrative account" based on our understanding of MAS' policy intent. Will this be correct? **3. Comments on the proposed cyber security requirements:** *(1) "A relevant entity must implement one or more firewalls at its network perimeter to restrict all unauthorised network traffic".*

S/N	Respondent	Feedback from respondent
		The term of “firewalls at network perimeter” means firewalls to segment the internal network from the public internet. For a Global Financial Institution, network traffic between FI entities (e.g. HO) would be considered as internal network traffic. As per the MAS TRM Guidelines, FI would deploy other similar measures (e.g. Network ACL), within internal networks to minimise the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network.” Is this the correct interpretation? *(2) “A relevant entity must implement multi-factor authentication for the following: … (b) all accounts on any system used by the relevant entity to access confidential information through the internet.”* Cloud solutions are now commonly used by FIs via internet. What would be MAS’ expectation on access to Cloud solutions? *(3) “Implement multi-factor authentication for the accounts as stated in the Notice. Examples include but are not limited to: … an account belonging to Human Resource Department that can be used to remotely access staff information through the internet.”* We would appreciate if MAS can clarify if "Remote access" means (i) access to our systems outside our "office" via internet (e.g. from home, from hotel during business trip) and/or (ii) access to our systems hosted by "cloud solution providers" via the internet in our office and/or outside our offices. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
114.	Anonymous	Confidential
115.	Anonymous	Confidential
116.	Anonymous	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** *“Administrative Account”* *(Page 6) “administrative account”, in relation to a system, means any user account that has full privileges and unrestricted access to the system;*

S/N	Respondent	Feedback from respondent
		We have the understanding that the intended scope of "administrative account" and "system" is for technical administrative accounts with full privileges and unrestricted access to infrastructure platforms including operating system and databases. We suggest for MAS to revise the definition to reflect on the intended scope. *"System"* *(Page 7) 'system', in relation to a relevant entity, means any hardware, software, network, or other information technology ("IT") component used by the relevant entity.* The term 'System' appears to be defined very broadly. Following the gist of the Consultation Paper, it appears that the intended focus is on the infrastructure parts of systems. Hence, we suggest for the Authority further refine the definition of 'System' to be more specific. Alternatively, the definition of "System" in MAS Notice 644 Technology Risk Management ("Notice 644") can be adopted for better clarity and consistency. For reference: MAS Notice 644 definition of system: "system" means any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure <u>"Confidential Information"</u> Page 6 defines confidential information as 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; For a) which is about customer information, for consistency, we suggest it to be aligned to the definition of "customer information" that is available in the Guidelines on Outsourcing. For b), our view is that this definition is overly broad which will be onerous for banks to implement. We respectfully suggest that b) to be removed from the scope. For reference: Guideline on Outsourcing definition of customer information: "customer information" means –

S/N	Respondent	Feedback from respondent
		(a) in relation to an approved exchange, recognised market operator, approved clearing house and recognised clearing house, "user information" as defined in section 2 of the SFA; (b) in relation to a licensed trade repository and licensed foreign trade repository, "user information" and "transaction information" as defined in section 2 of the SFA; or (c) in the case of any other institution, information that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the financial institutions, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred; <u>"Critical System "</u> We suggest adopting the same definition in Notice 644 for better clarity and consistency. For reference: MAS Notice 644 definition of Critical System: "critical system" in relation to a bank, means a system, the failure of which will cause significant disruption to the operations of the bank or materially impact the bank's service to its customers, such as a system which— (a) processes transactions that are time critical; or (b) provides essential services to customers; <u>"Security Standard "</u> *(Page 7) "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;* The term "standard" as defined here could potentially be misunderstood. We recommend the Authority change it to "security configuration baseline". We also suggest for the removal of "procedures" from the definition so as to focus on the intended technical control. In the section of Proposed Cyber Hygiene Practices, we recommend to enhance the requirements using a risk based approach as there could be situations where the configuration baseline may not be feasible to be implemented 100% or other control mechanisms may lead to an acceptable residual risk. A risk based approach would strengthen the overall objective of securing the FI, while allowing appropriate levels of flexibility for customer-oriented innovation in the Financial industry.

S/N	Respondent	Feedback from respondent
		3. Comments on the proposed cyber security requirements: “Administrative Accounts” *A relevant entity must secure every administrative account on its system to prevent any unauthorised access to or use of, such account.* The phrases “must secure every administrative account” and “to prevent any unauthorized access to or use of” indicate a rigid requirement to the relevant entity, without regard to whether the actual impact and residual risks are big or small. We recommend the Authority to enhance this statement with the term “with reasonable measures put in place by the FIs to protect against any unauthorized access of such account”. This would be better aligned to the intended security objective of protection and risk-based measures. “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.* We recommend the Authority apply the risk based approach to patching as well. Patching in a FI environment can be challenging. Even if a patch is available, it might not be possible to apply it without causing instability or incompatibilities to the system. In such cases, the FIs should conduct a risk assessment and seek measures to reduce the risks to an acceptable level. In this connection, we suggest the Authority further refine this requirement with a risk based approach. “Firewall” *A relevant entity must implement one or more firewalls at its network perimeter to restrict all unauthorised network traffic.* Firewall is one specific type of security devices used to secure network access. We recommend the Authority to consider the overall objective and to use the term “Network Access Control” instead as it can more broadly and better represent this security control. “Anti-virus”

S/N	Respondent	Feedback from respondent
		A relevant entity must implement one or more anti-virus measures, to mitigate the risk of malware infection on its system. Other than anti-virus, there are also other security measures to address malware risk such as HIPS, APT, etc. Therefore, we suggest the Authority to define this control in a broader way to encompass the other security measures. “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.* *Annex B 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.* With reference to (a) and the example provided in Annex B Para 9, it might be good to aim for consistency and use ‘administrative account’ when referring to technical administrative accounts with full privileges and unrestricted access to infrastructure platforms including operating system and databases. For (a), our recommendation is to define this control as only applicable for administrative accounts requiring human interactive login. Multi-factor control is often not feasible for accounts used for most automated system-to-system communications. For (b), referring to our comments on the definition of “confidential information”, we suggest that the samples listed in Annex B Para 9 to be aligned for consistency. With this, the sample about Human Resource department should be removed from the paper. We suggest for the Authority to allow the FI to determine which accounts and systems based on a risk-based approach.

S/N	Respondent	Feedback from respondent
		Furthermore, we are of the opinion that this should only apply to systems owned by the relevant entity and it should only apply to end user accounts where feasible and following the relevant entity's own risk-based assessment. Additionally, in view that detection is a key cyber defence function, the notice should consider having the FI to ensure that there is adequate logging and monitoring of system and user activities. **4. Comments on the proposed transition period:** Our recommendation is to set a transition period longer than 18 months as this Notice's requirements can be quite far-reaching. The Bank might not be able to fulfil the proposed 12 months transition period due to the Bank's large and complex infrastructure setup and wide geographical presence, coupled with the complexity of the Notice's broad scope and definitions. **5. General Comments:** Overall, we recommend to further refine the Notice to be more descriptive and follow a risk-based approach so as to better assist the FIs in operationalising this Notice.
117.	Leon Tham	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** I would like to suggest to MAS to consider the definition that holding the phone itself would satisfy the "something you have" portion of the security trio, and the passcode or fingerprint unlock would satisfy the "something you know" or "something you are" portion. With the implementation of application passwords, that would mean only that particular phone could access that email account as well. In conclusion, I hope that MAS takes the definition above and allow emails on phone to function without the need to login everything. **3. Comments on the proposed cyber security requirements:** No comments. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.

S/N	Respondent	Feedback from respondent
118.	Anonymous	Confidential
119.	Anonymous	Confidential
120.	World Federation of Exchanges	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** Standard definitions should be used instead of forming new ones in order to maintain consistency and avoid confusion across the industry. The WFE suggests using established definitions e.g. from NIST: https://csrc.nist.gov/glossary / https://nvd.nist.gov/800-53/Rev4. The NIST approach to cyber security in the last number of years has been pragmatic, timely, and has become dominant in the industry. We also note the following Control Families from NIST for consideration: AC - Access Control AU - Audit and Accountability AT - Awareness and Training CM - Configuration Management CP - Contingency Planning IA - Identification and Authentication IR - Incident Response MA - Maintenance MP - Media Protection PS - Personnel Security PE - Physical and Environmental Protection PL - Planning PM - Program Management RA - Risk Assessment CA - Security Assessment and Authorization SC - System and Communications Protection SI - System and Information Integrity SA - System and Services Acquisition − System: The definition of “systems” should include technology services, and include “enterprise environment” or alternatively define the system as comprising of sub-systems that form the enterprise architecture of an organisation. − Confidential Information: The definition of “confidential information” is broad and open to interpretation, and potentially covers a wide array of internal information including customer comments, feedback, phone directories and so on. Given that financial institutions (FIs) are already required to implement 2FA to secure such information, the definition needs

S/N	Respondent	Feedback from respondent
		to be further tightened. MAS should consider defining “confidential information” by referencing existing regulations, such as, SFA/SFR, PDPA. − <u>Vulnerability</u>: The proposed definition of “vulnerability” is incomplete. For example, system weakness could be exploited to deny the use of the systems or compromise the availability or integrity of the system and data. MAS should consider other established references, e.g. FSB drafted Cyber Lexicon. **3. Comments on the proposed cyber security requirements:** − <u>Security Patches</u>: We note that the systematic assessment of the patches that is suggested in the proposal is time consuming "...within a timeframe that is commensurate with the risks posed by such vulnerabilities…" We suggest as a more workable approach that system criticality should be patched first, and then later the other systems; otherwise, vulnerability risks should be used as the criteria to see how quickly systems should be patched. Generally, CIRT teams, operations teams and security teams define the critically of patches for systems (particularly internet-facing applications). Patching should follow a standard risk-oriented approach. While patching is an important part of cyber hygiene, over-reliance should be avoided since zero-day vulnerabilities by definition prove that there will always be situations where systems are not patchable. As such, we propose that the MAS focus on the organisational basics that will prevent or limit the impact of compromise in a world where atomic vulnerabilities and exploits will come and go. We also propose that the MAS offers a guideline on what constitutes a reasonable timeframe for applying the patches. We note if patching cannot be applied, then the MAS should suggest the use of plans of action and milestones (POA&M) within a formal process for risk acceptance. This is also in line with the FISMA Risk Management Framework (RMF) best practices and could simply be applied to the financial industry. Security patches are also part of the vulnerability management process which encompasses more than security patches. As such, we also suggest the MAS may want to focus more on the vulnerability management program; and under vulnerability management, focus on process development, policies and technology implementation.

S/N	Respondent	Feedback from respondent
		− Security Standards: Instead of prescribed standards, we note that a framework for setting standards may be more effective, as writing and maintaining a more detailed set of security standards for the system prove too inflexible. This would free up time to: o Understand the business value of a specific system as well as related potential impacts and risks of security breaches. o Maintain the security of the system. o Business lines should define risk appetite within the standards, for example the business would define how often internet-facing application should be pen tested (which, depending on the application's significance, could be anything from once a year to never). o Monitor conformance with the standards. We also note that it will be good if the MAS can set out the expectation of the high-level technical configuration that should go into the security standard. For example, the CSA Cybersecurity Code of Practice states: The security baseline configuration standards shall address the following security principles: a. Least access privilege and separation of duties; b. Enforcement of password complexities and policies; c. Removal of unused accounts; d. Removal of unnecessary services and applications, e.g. removal of compilers and vendor support applications; e. Closure of unused network port; f. Protection against malwares; and g. Timely update of software and security patches that are approved by system vendors. − Firewalls: We note that firewall rules should be reviewed on a regular basis. We suggest emphasising the desired functionality and impact of a firewall, as opposed to focusing on the mere existence of one. Outbound access to the Internet from data-centre systems should be eliminated, since this might lead to the establishment of command and control persistence, additional malware installation, and data exfiltration. Outbound access is a core concept that does not ebb and flow with software deployments and patches, and there is no zero-day threat to this type of control. With respect to inbound access, specific services and destinations should be defined and authorised, but all other access should not be possible. Networks should be segmented

S/N	Respondent	Feedback from respondent
		into security zones, and lateral movement among those zones should be restricted to only known and authorised connections. Finally, end-user/employee Internet access should be explicitly addressed with a specification that inbound access to these networks should be absolutely and completely denied from the internet other than specific authorised VPN services, and outbound access should implement content filtering and restricted services, such that only authorised uses and protocols are permitted. − Anti-virus: Given that "system" is defined as any hardware, software, network, or other information technology component used by the relevant entity, anti-virus measures are not applicable to some of the components. Hence, we would like to propose "A relevant entity must implement one or more anti-virus measures where applicable, to mitigate the risk of malware infection on its system." − Multi-factor Authentication: Section 9(b) requires MFA for "all accounts on any system". As organisations cannot implement MFA on systems they do not own, we would like to propose "all accounts on its any system used by the relevant entity to access confidential information through the internet." SUGGESTED ADDITIONS TO THE PROPOSAL: − Regular penetration testing of all critical systems – whether they face the internet or not – should be added to the proposal. This would help to reduce the risk of internal attacks or implanted malware (e.g. Bank of Bangladesh, Vietnam). Additionally, the approach should be risk-oriented, focusing on Internet facing applications first, then other critical applications, as well as demand given by business functions. − Testing: Regular testing should be implemented to cover vulnerability scanning, with a focus on internet-accessible hosts. Scenario-based testing should be implemented to emulate adversaries that have compromised similar business using identified techniques and tactics, with a feedback cycle to remediate discovered weaknesses. User education and testing should be used to measure and improve susceptibility to social-engineering attacks such as phishing. We also suggest adding a quarterly review of all IT infrastructure business applications, user accounts, and removal of accounts that no longer meet the requirements of the standard.

S/N	Respondent	Feedback from respondent
		− Behavioural detection: We suggest adding a regular review of logs, potentially using machine learning tools, to point to suspicious and malicious activities. We also suggest moving away from a tickbox human "review" of firewall logs, which is considered near impossible to perform effectively. − E-mail hygiene: Education and technical controls should be implemented to mitigate risks carried via e-mail, including phishing links, malicious attachments, and "narrative attacks" that establish false rapport with employees as a precursor to fooling employees into unauthorised actions such as wire transfers. The programme should include education, regular phish testing, and mail filter controls that identify and prevent common malicious campaigns. − Information sharing: Organisations should take advantage of sector or region-specific trust-based groups to share and receive threat intelligence and gain awareness of specific threats, campaigns, and countermeasures. **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.
121.	MUFG (Securities) Asia (Singapore	**1. Comments on the applicability of the Notice:** No comments. **2. Comments on the proposed definitions:** No comments **3. Comments on the proposed cyber security requirements:** in relation to the requirements on multi factor authentication placed on cloud solution providers. We would like to know whether Cloud Solution providers are required to meet the MAS' multi factor authentication requirements. Currently, there are controls in place such as IP restrictions to prevent access via Public Network. Where access via internet is from the office, does the provider needs to adhere to the multi factor authentication? **4. Comments on the proposed transition period:** No comments. **5. General Comments:** No comments.

S/N	Respondent	Feedback from respondent
122.		**1. Comments on the applicability of the Notice:** 1.1 Microsoft would like to thank MAS for the opportunity to provide comments on the proposed Notice on Cyber Hygiene ("Notice"). Microsoft supports the initiative to develop broadly applicable baseline cybersecurity requirements to help ensure the overall security of the ecosystem. We agree with MAS's observation that "many of the cyber breaches which occurred globally were often due to poor cyber hygiene." Microsoft receives 6.5 trillion signals per day through its intelligent security graph, which serves as the foundation for all of Microsoft's security solutions, obtaining threat signals from Microsoft's services, expansive user base, and global footprint . Anonymized information relating to infected computers that is received as a part of this process shows that the failure to patch, even years after a patch has been issued, is prevalent across Asia. The use of pirated software brings even more risk, as a National University of Singapore study conducted on behalf of Microsoft showed in 2017 . 1.2 We support MAS's approach in setting forth baseline requirements and mapping those to a list of non-mandatory potential implementation measures which may be applicable to different relevant entities. This approach helps ensure that the Notice is not overly prescriptive. At the same time, the Notice could be even more outcomes-focused to ensure that it will accommodate a range of technical alternatives that could support the same outcome, and account for the broad range of financial institutions to which the Notice applies. We have found that outcomes-focused approaches "enable organizations to engage a broader internal audience, including executives" and "allow for greater flexibility in adjusting and improving how organizations manage, upgrade, and develop new security techniques." For example, instead of requiring a firewall specifically, the practice could be described in terms of the objective, e.g., "network defense." That way, a relevant entity can consider other means of protecting the network perimeter, and, as new and more effective protection measures are developed, they can be implemented without the necessity of MAS updating its requirements. Firewalls may be given as an example, as they are important technology today. Supplemental examples of today's technology could include Intrusion Detection Systems and other cyber threat indicators. Please refer to our comments on specific Cyber Hygiene Practices below.

S/N	Respondent	Feedback from respondent
		1.3 We also support the risk-based approach in the Notice, as exemplified in the sections on Security Patches, Security Standards and Anti-Virus in particular. With this approach it may be worth considering adding some Cyber Hygiene Practices around governance and/or risk assessment. Please refer to our comments in Section 3 below. **2. Comments on the proposed definitions:** 2.1 The definition of "confidential information" seems overly broad. ISO 27000:2018 defines confidentiality as the "property that information is not made available to unauthorized individuals, entities, or processes." Using that concept, the definition could be revised to "(a) any customer information that is only made available to authorized individuals, entities, or processes; and (b) any information relating or belonging to the relevant entity that is only made available to authorized individuals, entities, or processes and that is not in the public domain." This seems more specific and clearer than information that "is not publicly available." 2.2 The definition of "critical system" includes systems which "provide[] essential services to customers." "Essential" is undefined and should be clarified, unless the intent is that the FI itself define what is "essential" (in which case we recommend that should be made clear). If "essential" is defined by MAS, we recommend that it be defined as: "core banking which includes back-end system that processes banking transactions across the various branches of a bank. The system essentially includes deposit, loan and credit processing. Among the integral core banking services are floating new accounts, servicing loans, calculating interests, processing deposits and withdrawals, and customer relationship management activities." 2.3 The definition of "vulnerability" is vague to the extent that it references "to compromise the security configuration settings of the system." We recommend changing the definition to "to defeat the controls used to protect confidentiality, integrity, or availability of an information system or its information." Considering this is a mandatory requirement we think this language is clearer and easier to assess compliance against. **3. Comments on the proposed cyber security requirements:** 3.1 Administrative Accounts: We do not have any suggested changes to this cyber hygiene practice as set forth on p.8. We have suggested an addition to the recommended implementation measures in Annex B that the number of

S/N	Respondent	Feedback from respondent
		administrative accounts should be restricted, administrative credentials should be restricted so that they may not be shared, and accounts with administrative privileges should only be used to perform administrative tasks. Standard accounts should be used for general work. Restricting accounts with administrative privileges reduces the chance that an administrative account will be compromised. 3.2 Security Patches: As noted above, Microsoft's Security Intelligence Graph and data relating to botnet take down operations demonstrates that failure to patch is the number one technology system vulnerability that is exploited by cybercriminals. Effective patch management must be mandated, although the mandate may be tailored to the severity of the threat from the unpatched software. This is especially important for entities that are using on premise software and, thus, do not benefit from patching performed by their cloud provider. As a component of this policy, we recommend advising against the use of pirated software and software that is no longer supported by virtue of its end of life. Accordingly we recommend adding a section 5(c) as follows: "Relevant entities must not use counterfeit or pirated software, or software that has reached its end of life in terms of manufacturer's support, due to the associated risks and lack of support." 3.3 Security Standards: While we appreciate that MAS is trying to avoid being overly prescriptive, it is unclear what is meant by "security standards." It may be helpful in Annex B to enumerate some topics that the standards might relate to, and provide a sample (non-mandatory) standard for reference, e.g., "Passwords must be at least X characters long and contains at least Y special characters." We further recommend that the security standards should include a security incident response plan and a governance process for regular risk assessment review. This could be part of the mandatory requirements in section 6 or added to Annex B as a recommendation. 3.4 Firewall: We recommend revising this Cyber Hygiene Practice to be more outcomes-focused, by changing it to "Network Defense: A relevant entity must implement network security measures, such as a firewall at its network perimeter and, if possible, network intrusion detection systems to restrict unauthorised network traffic."

S/N	Respondent	Feedback from respondent
		3.5 Anti-virus: Similarly, we recommend revising this Cyber Hygiene Practice as follows: "Protection against Malware: A relevant entity must implement measures to mitigate the risk of malware infection on its system(s), such as anti-virus measures and intrusion detection systems." **4. Comments on the proposed transition period:** The proposed effective date seems acceptable, given the requirements are minimal and that relevant entities are likely to have many of the measures in place already. **5. General Comments:** 1.1 The notice is technology neutral. While we generally support this approach, it may be worth distinguishing between on-premises and cloud-based systems because of the shared responsibility involved with outsourced cloud services. It may help to refer to the Outsourcing and Technology Risk Management Guidelines and to make clear that certain practices, such as patching, are particularly important for on-premises systems. It would also be helpful in the preface to the notice to clarify that the Notice applies regardless of the technology used. 1.2 We support the inclusion of Annex B which suggests various means of implementing the required measures. We recommend the following additions to Annex B: • Add to Administrative Accounts: "Restrict the number of administrative accounts and ensure the accounts are used only to perform administrative tasks and are blocked from accessing email or the Internet." Also, it should be made clear that administrative account credentials should not be shared among people accessing a particular account, as this impacts the ability to audit access of a particular account. Finally, we recommend that the last bullet in this section recommend that they regularly conduct audits to assess whether those with administrative access are still in need of such access in order to perform their duties. • Add to Security Patch: With respect to the second bullet point, we recommend a time recommendation within which relevant entities should assess the criticality of a patch, such as recommending that they "Establish and enforce a policy to evaluate the criticality of a security patch within X hours of release. High priority patches should be installed as soon as possible and, in any event, within Y hours of release unless the patch cannot be applied due to critical functionality issues."

S/N	Respondent	Feedback from respondent
		• In addition, we recommend that the last bullet be revised as follows: "The framework should include controls and technological defences, such as intrusion detection systems and network segmentation, to reduce any risk in the event that a patch cannot be applied" (suggested changes italicized). • Security Standards: As noted above, we recommend adding an example to clarify what is meant by a "security standard" and what types of topics might be covered. In addition, we recommend including security incident response plans and governance processes to review risk assessments as topics that should be covered by security standards. • Multi-Factor Authentication: We recommend using multi-factor authentication for all employee accounts, especially if employees are permitted to access the covered entities' corporate networks while away from the office. MAS may want to consider including additional recommendations or best practices in Annex B. We recommend that MAS refer to the following standards and materials, if it has not already: ISO/IEC 27103, which depicts a cybersecurity risk management approach that is consistent with the NIST Cybersecurity Framework and in-development financial services sector-specific cybersecurity framework profile; ISO/IEC 27001, a widely used international standard that's integrated with ISO/IEC 27103; and the Center for Internet Security's Top 20, a set of industry-developed guidance that is referenced in the NIST Cybersecurity Framework. 1.3 We are strongly supportive of MAS's initiative in setting forth baseline mandatory cybersecurity measures for the financial services sector and would welcome the opportunity to engage further and partner with MAS, and other parts of the Singapore government, to increase awareness and enhance cybersecurity. To the extent possible, it would be beneficial to ensure these baselines are in harmony with those that are already in place in other geographies to maximize ease of compliance for multi-national FIs. Use of international and/or industry-developed standards or compatibility with international standards-based approaches, including those referenced above, helps to ensure such consistency and interoperability.
123.	CREST GB Ltd	Confidential

MAS

Monetary Authority of Singapore