RESPONSE TO FEEDBACK RECEIVED – CONSULTATION PAPER ON THE TECHNOLOGY RISK MANAGEMENT GUIDELINES

1 Introduction

1.1 On 13 June 2012, MAS conducted a consultation on the Technology Risk Management Guidelines, (the "Guidelines"). The Guidelines include guidance on existing and emerging technology trends and security concerns in the financial industry. In addition, several IT circulars have been subsumed into the Guidelines for ease of reference.

1.2 MAS sought public feedback on 5 areas: data centres protection and controls, mobile banking and payment security, payment card system and ATM security, combating cyber threats; and customer protection and education. We have consolidated the feedback and provided our response in this paper.

1.3 The public has also provided feedback on other topics in the Guidelines where feedback was not sought. Where applicable, MAS has responded in this paper to feedback which reflected common concerns.

1.4 The consultation closed on 16 July 2012. All feedback has been carefully considered and we thank all respondents for their valuable feedback and comments. As many respondents have requested for confidentiality, MAS will not be publishing the list of respondents.

2 Chapter 10 - Data Centres ("DCs") Protection and Controls

2.1 MAS' Definition of "Critical" (paragraph 10.0.1)

2.1.1 One respondent asked how MAS defines the term "critical", and sought guidance on the kind of application, system, network device and data MAS will consider as "critical".

MAS' Response

2.1.2 The Notice on Technology Risk Management (the "Notice") defines a "critical system" as any system, the failure of which will cause significant disruption to the operations of the financial institution ("FI") or materially impacts the FI's service to its customers. Each FI would need to assess and identify which systems are critical, according to its business operations.

2.2 **Responsibility for performing of Threat and Vulnerability Risk Assessment (TVRA) (section 10.1)**

2.2.1 Several respondents asked whether TVRA for data centres ("DC") should be performed by FIs, DC service providers, or DC owners.

MAS' Response

2.2.2 FIs are responsible for ensuring that TVRAs are performed for their DCs. An FI may appoint a third party or its employees with the requisite knowledge and qualifications to perform a TVRA on the DC facility.

2.3 **Scope and Frequency of TVRA on DC (paragraphs 10.1.2, 10.1.3 and 10.1.4)**

2.3.1 Some respondents asked MAS to provide more guidance on the scope of TVRAs and the expected frequency of TVRA reviews. Respondents also asked:

a) Whether reviewing a TVRA report onsite at the DC facility is sufficient to meet regulatory expectation;
b) Whether the scope of TVRAs should include natural disasters, as well as the political and economic climate of the country in which the DC facility resides; and
c) Whether the scope of TVRAs should include the DC facility's perimeter and surrounding environment.

MAS' Response

2.3.2 It is neither appropriate nor possible for MAS to prescribe an exhaustive set of specifications on TVRA as the scope of assessment is dependent on many factors such as the criticality and the type of systems hosted at the DC. Nevertheless, the scope of a TVRA should minimally include the DC's perimeter, physical and environmental security, natural disasters, and the political and economic climate of the country in which the DC resides.

2.3.3 MAS expects FIs to perform a TVRA on the DC facility before procuring the DC services and to ensure that all identified risks are adequately addressed. This can also be achieved by obtaining and reviewing a current TVRA report from the DC service provider. Subsequent assessments should be conducted at a frequency that

is commensurate with the level and type of risk to which a DC is exposed as well as the criticality of the DC to the FI.

2.4 **MAS' Definition of DC and When Threat Vulnerability Risk Assessment is Applicable (paragraph 10.1.1)**

2.4.1 Several respondents asked how MAS defines "Data Centre" and whether MAS' expectation on TVRAs applies to computer or server rooms.

2.4.2 Some respondents also asked whether MAS expects a TVRA to be performed on both onshore and offshore DCs, and DCs hosting non-critical systems. One respondent highlighted that not all FIs will have the contractual right to obtain a TVRA report from their DC service provider given the sensitive nature of the information in the reports.

2.4.3 A respondent suggested that FIs should form a committee comprising qualified security consultants to determine the type and level of protection that should be established to safeguard DCs.

MAS' Response

2.4.4 A DC is a physical facility that houses physical IT infrastructure and equipment; and includes computer and server rooms. MAS expects FIs to perform TVRA on DCs regardless of whether they are located in Singapore or overseas, as long as the DCs support FIs' Singapore operations.

2.4.5 FIs should ensure that DC service providers are able to provide FIs with adequate information to facilitate their risk assessment.

2.4.6 Where applicable, FIs may collaborate to determine the type and level of protection needed to safeguard DCs as long as the assessment meets the expectations in the Guidelines.

2.5 **Threat Vulnerability Risk Assessment (paragraph 10.1.1)**

2.5.1 A respondent commented that TVRAs should focus on impact assessment and risk management rather than on threat scenarios.

MAS Response

2.5.2 The objective of a TVRA is to identify security threats and operational weaknesses in a DC in order to determine the type and level of protection that should be established to safeguard it. Hence, a TVRA should factor in possible scenarios of threats as part of an FI's impact assessment and risk management of its DC.

2.6 **DC Physical and Environmental Controls (sections 10.2 and 10.3)**

2.6.1 Many respondents asked whether MAS can define the requirements on DC security in detail. Other respondents suggested that guidelines such as on the retention of access logs and CCTV recordings, adoption of ISO standards, and auto corrective mechanical and engineering controls be included in the Guidelines. One respondent also asked whether non-DC personnel should be accompanied at all times by a DC staff.

MAS' Response

2.6.2 It is not MAS' intention to require FIs to adhere to a specific set of DC security controls and standards. MAS' objective is to provide guidance on the key areas in DC security which FIs should include as part of their technology risk management.

2.6.3 FIs are expected to perform proper due diligence in identifying and implementing the controls, processes and procedures to manage DC security.

2.6.4 FIs should ensure that visitors are accompanied at all times by an authorised staff while in the DC.

3 **Chapter 12.2 - Mobile Online Services and Payments Security**

3.1 **Mobile Banking Services and Near-Field Communication ("NFC") Technology (paragraphs 12.2.1 and 12.2.2)**

3.1.1 A few respondents enquired whether this paragraph implies an expectation from MAS for FIs to offer mobile payment services and NFC technology.

MAS' Response

3.1.2 The offering of mobile payment services and NFC is a commercial decision to be made by an FI. FIs should conduct their risk assessments before adopting new technologies such as near-field communication.

3.2 **Mobile Online Services and Payments Security (paragraph 12.2.3)**

3.2.1 A respondent suggested excluding the need for two-factor authentication for mobile payments which are not performed using a bank account such as those using stored value facility.

3.2.2 Another respondent suggested defining the frequency of risk assessment for mobile online services and payment.

MAS' Response

3.2.3 MAS expects FIs to provide a safe environment for customers to conduct financial services on the mobile platform. The security controls which are defined for online financial services are applicable to applications accessible via mobile devices. Two-factor authentication is required for all logins and sensitive transactions performed over the internet using mobile devices.

3.2.4 MAS does not prescribe the frequency of conducting risk assessment for mobile online services and payment. FIs should determine the frequency based on their evaluation of the risks to which the mobile online services are exposed.

3.3 **Verification of Integrity and Authenticity of Downloaded Application (paragraph 12.2.4)**

3.3.1 Some respondents commented that it may not be necessary for FIs to ensure that customers are able to verify the integrity and authenticity of the FIs' applications before downloading them, given the implementation of two-factor authentication and transaction signing.

3.3.2 Several respondents sought clarification on the means to perform integrity and authenticity verification of downloaded applications. A respondent suggested that each FI should be able to uniquely identify the customer's mobile phone using technology such as IMEI or some other unique identification number, make and model number when the FI provides mobile online services to the customer. The respondent, together with other respondents, further suggested that FIs should implement additional requirements (such as session timeout, memory clearing, adequate passwords or PINs handling, jailbreak prevention and detection, remote data wiping etc) on their mobile applications to strengthen the security of mobile online services.

MAS' Response

3.3.3 MAS has considered and accepted the respondents' suggestion to remove the need for FIs to ensure that customers are able to verify the integrity and authenticity of the applications before downloading them, given the implementation of two-factor authentication and transaction signing.

3.3.4 MAS expects FIs to provide a safe environment for customers to conduct financial services on the mobile platform. Hence, security controls, such as session timeouts, which are defined for online financial services in the Guidelines, are also applicable for applications accessible via mobile devices.

3.4 **Encryption of Sensitive Data (paragraph 12.2.5)**

3.4.1 A respondent expressed concern that encryption may not be possible for data that is stored on the customer's device. Another respondent highlighted that the feasibility of implementing encryption on each customer's device is dependent on the device's capability.

3.4.2 Another respondent highlighted that it is not possible for data to be encrypted during processing.

3.4.3 A respondent requested for a clearer definition of "confidential data".

MAS' Response

3.4.4 The mobile application provided by each FI should protect information that is exchanged between the customer via a mobile device and the FI. The security controls implemented by the FI to protect sensitive information should be supported by the mobile device.

3.4.5 MAS agrees with the respondent's feedback that it is not possible to process encrypted data. The confidentiality and integrity of data should be adequately protected while the data is being stored in systems, transmitted across networks and being processed. To achieve this, FIs are expected to protect sensitive or confidential data with strong encryption during transmission and in storage. Such data should only be in the clear when it is processed in a secure environment such as the Hardware Security Module. The Guidelines has been revised to provide better clarity.

3.4.6 Generally, customer personal information, identity details and transaction data are considered as "confidential". As different FIs store and process different types of data, MAS expects FIs to determine the information which is deemed "confidential" to their organisations and business.

3.5 **Scope and Frequency of Customer Education on Protecting Personal Mobile Device (paragraph 12.2.6)**

3.5.1 A respondent highlighted that each FI should not be responsible for educating its customers regarding protection of their mobile devices from theft and loss. There was also feedback which proposed the customer education programme to be conducted at the national level.

3.5.2 Another respondent suggested implementing customer education programmes on a periodic instead of on a continuous basis, while another respondent enquired on the scope and delivery channel for customer education programmes.

MAS' Response

3.5.3 MAS expects FIs to design and deliver an adequate customer education programme. Similar to internet banking, it is important that FIs provide sufficient information on IT security risks to and share best security practices with its customers, as part of its customer protection programme.

3.5.4 With regard to the feedback on the frequency of customer education programmes, MAS' view is that continual education, such as posting of educational materials on IT security and security alerts on the FI's website, is necessary to educate its customers on the risks of using online financial services and to explain the security controls implemented by the FI to protect its customers. FIs may wish to conduct consumer education programmes through their respective associations.

4 Chapter 13 - Payment Card Security

4.1 Payment Card Security (Chapter 13)

4.1.1 One respondent suggested including a section on contactless card security control expectations.

4.1.2 Another respondent suggested that this section should not apply to FIs that utilise, but do not own, the payment card infrastructure.

MAS' Response

4.1.3 Guidance in the payment card security section is applicable to both contact and contactless cards. FIs are expected to assess their payment infrastructures and implement adequate security controls to combat payment card fraud for both types of cards.

4.1.4 The Guidelines are applicable to FIs which own or utilise a payment card infrastructure. FIs which utilise a third party payment card infrastructure should assess the adequacy of the service provider's internal controls, processes and procedures. FIs are accountable for the security and availability of payment card services provided to their customers.

4.2 Payment Card Fraud (section 13.1)

4.2.1 A respondent suggested that the mobile operator and application provider should not be responsible for performing security checks on applications such as mobile wallets.

MAS' Response

4.2.2 MAS notes the feedback from the respondent. FIs are expected to assess and implement security measures over the solutions they have deployed or outsourced.

4.3 **Online Transaction Authorisation (paragraphs 13.1.1, 13.1.2 and 13.1.3)**

4.3.1 Some respondents enquired if the online transaction authorisation requirement applied only to transactions made in Singapore.

4.3.2 Some respondents sought clarification on the types of payment card data that need to be encrypted. One respondent suggested encryption for all payment card data.

MAS' Response

4.3.3 Online transaction authorisation is applicable for all payment cards issued to Singapore customers, regardless of where the transactions are made.

4.3.4 MAS expects each FI to perform its risk assessment to determine the type of payment card data which should be encrypted. MAS also expects confidentiality and integrity of sensitive payment card data to be adequately protected by the FIs while the data is stored on cards, in systems, transmitted across networks and being processed.

4.4 **Card Authentication Mechanisms (paragraphs 13.1.2 and 13.1.3)**

4.4.1 A respondent sought clarification on whether dynamic data authentication (DDA) or combined data authentication (CDA) are meant for authentication for offline card use. The respondent further enquired whether the magnetic stripe can be used to store sensitive payment card data since overseas ATM withdrawals may still rely on the magnetic stripe. Another respondent enquired whether offline authentication is required if online authentication is always performed for all card transactions.

4.4.2 In addition, a respondent sought clarification on whether offline card authentication is allowed for emergency cases. Another respondent enquired whether card authentication and transaction authorisation can be performed by an affiliate of the FI.

MAS' Response

4.4.3 Card authentication methods such as DDA and CDA support both online and offline card authentication.

4.4.4 Sensitive information will continue to be stored on magnetic stripes as long as overseas ATM withdrawals rely on the information residing on magnetic stripes to perform card authentication. Hence, banks are expected to put in place the necessary security to protect their customers' bank accounts. These include disabling overseas withdrawals unless requested by the customer, SMS alerts for cash withdrawals above a certain threshold, and replacing ATM cards that are assessed to be at risk. Banks are also expected to strengthen their fraud surveillance capability.

4.4.5 Offline card authentication is allowed for credit and debit cards when online card authentication is unavailable. However, online authentication must be performed for transactions using ATM cards. Offline authentication is not allowed for ATM card transactions.

4.4.6 Card authentication and transaction authorisation, should be performed by the card issuer or its affiliates.

4.5 **System Security Control Version (paragraph 13.1.4)**

4.5.1 Two respondents requested MAS to provide guidance on the security patch, system patch or upgrade version that should be implemented on payment card systems.

MAS' Response

4.5.2 FIs are expected to establish a process to identify, assess, test and deploy new system patches, security patches or upgrades to protect their payment cards and other systems from fraud. This guidance has been moved from paragraph 13.1.4 to patch management under Section 9.5 of the Guidelines.

4.6 **Payment Card Security Controls (paragraph 13.1.5)**

4.6.1 A respondent enquired whether the two statements stipulated in this paragraph "New payment cards sent to customers via post should only be activated upon obtaining the customer's instruction. A dynamic one-time-password (OTP) should also be implemented for card not present (CNP) transactions via the internet to reduce fraud risk associated with CNP" are linked and if so, the implications envisaged by MAS.

MAS' Response

4.6.2 These two statements set out two security controls required to mitigate the risk of payment card fraud at card issuance and for CNP transactions. MAS has revised these statements for clarity.

4.7 **Transaction Alert (paragraph 13.1.6)**

4.7.1 A respondent enquired on the mode of communication that is fit for sending transaction alerts.

4.7.2 The respondent also asked for advice on how the customer can check and change the customer-defined threshold. It was suggested that the transaction alert threshold be stated on payment card statements.

MAS' Response

4.7.3 MAS does not prescribe the mode of communication for delivering transaction alerts. FIs are expected to perform their risk assessments and determine the adequate modes of communication for delivering transaction alerts.

4.7.4 FIs are also expected to implement functions for customers to check and change the threshold limits. Sufficient security controls should be implemented for users to access these functions.

4.8 **Fraud Detection System (paragraph 13.1.7)**

4.8.1 A respondent suggested that a fraud detection system that has a function which is equivalent to behaviour scoring systems should be allowed as long as the system has the capability to identify and curb fraudulent activities. Another respondent enquired on the expectations of the algorithms that are used for behavioural scoring and correlation.

MAS' Response

4.8.2 MAS has updated the Guidelines to accept fraud detection systems that are equivalent to behaviour scoring systems.

4.8.3 Each FI is expected to identify and configure the scoring parameters according to its risk assessment of its payment card base.

4.9 **Follow-up Action for Suspicious Transactions (paragraph 13.1.8)**

4.9.1 A respondent suggested that FIs should only institute follow up actions for high-risk transactions, instead of all transactions, which exhibit behaviour that deviates significantly from a cardholder's usual card usage patterns.

4.9.2 Another respondent suggested that to enhance customer education and to provide assurance to customers that FIs are concerned about card security, MAS can direct each FI to share the follow up actions taken to address deviations from any customer's usual card usage patterns.

MAS' Response

4.9.3 MAS expects FIs to implement a framework and measures to identity and handle transactions that do not match a cardholder's usual card usage patterns. This is to enable the FIs to take early and swift action to curtail card fraud.

4.9.4 FIs are also expected to implement a customer education programme to help cardholders understand the different controls which have been implemented to reduce fraudulent transactions. MAS will work with the industry to ensure that adequate information on card security is disclosed to cardholders in a timely manner.

4.10 **ATM and Payment Kiosks Security (section 13.2)**

4.10.1 A respondent suggested including more security controls for ATMs. These controls include access control policy and IT audit expectations. Another respondent sought clarification on the need to implement security controls at ATMs since magnetic-stripe transactions are no longer accepted in Singapore. Many respondents enquired about the expected controls on ATMs, including foreign device detection, detection mechanisms and alerts, two-factor authentication as well as ATM physical security.

MAS' Response

4.10.2 The general guidance on IT security controls, set out in the Guidelines, is applicable to ATM systems. MAS expects FIs to implement adequate controls, processes and procedures to combat against ATM card fraud and ensure service availability.

4.10.3 While information on magnetic stripes will no longer be used to authenticate cards which are issued and used in Singapore, such information can be skimmed at the ATMs and used in countries that accept magnetic stripe cards. Card-issuing FIs should therefore implement sufficient security controls at ATMs.

4.10.4 FIs are expected to determine the controls, processes and procedures needed to provide adequate protection for ATM services. Depending on the design and location of the ATMs, such measures may include foreign device detection, fraud detection mechanisms and alerts, surveillance cameras, as well as other ATM physical security.

4.11 **Tamper-Resistant Keypads (paragraph 13.2.2(c))**

4.11.1 A few respondents enquired about MAS' expectation of tamper-resistant keypads as well as how this can be implemented. One respondent commented that it is not possible to implement "tamper-resistant keypads to ensure that no one can

identify which buttons are being pressed by customers" as stated in paragraph13.2.2(c). This is because PINs can be captured via video recording and thermal and infra-red imaging.

MAS' Response

4.11.2 Tamper-resistant keypads refer to keypads with the capability to encrypt the PINs at entry so that the PIN is protected during transmission from the keypad to the authentication servers. MAS notes the feedback and has revised the Guidelines for clarity.

5 Appendix E - Security Measures for Online Systems

5.1 Security Measures for internet-facing Systems (Appendix E)

5.1.1 A respondent suggested revising the appendix title to "Security Measures for Internet-Facing Systems".

5.1.2 Some respondents also enquired whether the expectations in Appendix E are only meant for retail banking.

MAS' Response

5.1.3 MAS will not be revising the title of Appendix E as these are guidelines for online financial systems.

5.1.4 Appendix E is not limited to retail banking as online financial services includes the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices.

5.2 Transaction Signing For Online Trading Systems and Mobile Devices (paragraph E.2.2)

5.2.1 Some respondents sought clarification on MAS' definition of "high-risk transactions" as well as the scope of transactions that require transaction signing. For example, there were questions on whether transaction signing is required for instructions placed in online trading systems and for transactions performed using mobile devices.

5.2.2 A respondent felt that the paragraph on the expectations of employing different cryptographic keys for the generation of OTPs and for transactions signing is unclear and requested for clarification.

5.2.3 Another respondent asked whether transaction signing is required for performing a change to customer details online. A respondent asked about the type of input that should be used for transaction signing. Lastly, two respondents expressed concern that customers will be confused over the use of transaction signing.

MAS' Response

5.2.4 FIs should perform a risk assessment to identify a list of high risk transactions. Some examples of high-risk transactions include changes to sensitive customer data, registration of third party payee details and revision of funds transfer limits. Transaction signing is required for all high-risk transactions performed via internet.

5.2.5 If a hardware token is used to generate an OTP and sign a transaction, the cryptographic key for generating the OTP should be different from the one used for transaction signing. If a cryptographic key is shared between the 2 functions, its compromise will impact both functions.

5.2.6 Amendment of personal details online should be allowed if transaction signing is implemented for this operation.

5.2.7 FIs should determine the type of input to be used for transaction signing. Generally, information which is unique to the transaction can be used for transaction signing.

5.3 OTP Time Window (paragraph E.2.3)

5.3.1 Two respondents suggested changing the time window from 100 seconds to 70 seconds and 180 seconds respectively. Another respondent enquired whether a 100-seconds time window is applicable for the SMS OTP.

MAS' Response

5.3.2 MAS has considered the respondents' comments and has revised the Guidelines to allow FIs to establish a time window that is as short as practicable to minimise the risk of the OTP being compromised. FIs are expected to perform a risk assessment on the duration of the time window and select the duration that is most appropriate for their services.

5.4 Convergence of Devices (paragraph E.2.4)

5.4.1 Many respondents asked whether SMS and email, available in a mobile device, are acceptable second channels for sending notification if the transactions are also performed on the same mobile devices. The respondents suggested allowing the notification to be sent to the customer on the same device that is used

to perform the transaction. Another respondent enquired whether over-the-counter transactions require notifications to be sent to customers.

MAS' Response

5.4.2 MAS understands that there are limitations for FIs to match the device where notification is received with the device from which transactions are performed. Hence, FIs should perform their risk assessments and implement controls that can address the risk arising from the same device being used to perform transactions and receive notifications. Adequate customer education should be provided to explain the attendant risks and the controls that FIs have instituted to address these risks.

5.4.3 MAS does not require notifications to be sent for over-the-counter transactions as FIs' personnel should have verified the identities of their customers when the transactions are performed at the FIs' premises.

5.5 **End-to-end Encryption (E2E) (paragraph E.2.5)**

5.5.1 A respondent sought clarification on whether E2E is applicable only to online financial services and whether E2E encryption should be implemented to protect PINS and passwords. Another respondent enquired if E2E encryption is applicable for outsourced online financial services.

MAS' Response

5.5.2 E2E encryption is required for online financial services, whether the systems are managed by the FI or outsourced to intra-group or third party service providers. Sensitive information such as customer PINs and passwords should be protected with E2E encryption.

5.6 **Session Time-out (paragraph E.2.6)**

5.6.1 A respondent enquired whether an OTP is required for re-authentication after each session time-out.

MAS' Response

5.6.2 All customers should be re-authenticated using two-factor authentication after each session time-out.

5.7 **Handling Secure Socket Layer (SSL) Server Certificate Warning (paragraph E.2.7)**

5.7.1 A respondent commented that mobile applications do not have the capability to detect and alert users to problems with SSL certificates. Another respondent enquired whether providing training and education materials to customers on handling SSL server certificate warnings is sufficient.

5.7.2 Another respondent highlighted that the FI should not be held responsible in the event that customers do not report issues with SSL certificates to the FI.

MAS' Response

5.7.3 Generally, web browsers on mobile devices have the capability to detect invalid digital SSL certificates and to display warnings.

5.7.4 Information on SSL certificate warnings should be part of the customer education provided by FIs.

5.7.5 The objective of this paragraph is to encourage FIs to provide sufficient information to their customers on handling SSL server certificate warnings, and also to encourage customers to report such issues to the FI.

6 Appendix F - Customer Protection and Education

6.1 Applicability of Appendix F on OTP, Non-Retail Customers, and New System Features (Appendix F)

6.1.1 One respondent asked MAS to clarify whether the expectations in Appendix F are applicable to static passwords and not OTPs. Another respondent asked whether the section on customer education (section F.3) and paragraph on session handling (paragraph F.2.6) are applicable only to retail customers.

6.1.2 One respondent also commented that the objective of paragraph F.3.2, "Customer education may include web-based online education or other media whereby a guided learning experience may be defined. When new operating features or functions, particularly those relating to security, integrity and authentication, are being introduced, FIs should ensure that customers have sufficient instruction and information to be able to properly utilise them. Continual education and timely information provided to customers will help them to understand security requirements and take appropriate steps in reporting security problems", is unclear.

MAS' Response

6.1.3 The paragraphs on password protection are for static passwords only.

6.1.4 Customer education should be provided to all customers, and not be confined to retail customers only.

6.1.5 The objective of paragraph F.3.2 is to provide guidance on the means through which customer education can be conducted and when customer education should be provided. MAS notes the feedback and has revised the paragraph for clarity.

6.2 **Verifying Authenticity and Integrity of Software used by Customers (paragraph F.2.1)**

6.2.1 Many respondents sought guidance from the Authority on how FIs can verify the authenticity and integrity of the software used by FIs' customers.

MAS' Response

6.2.2 The objective of the paragraph is for FIs to establish appropriate controls and processes to ensure the integrity of their applications that are implemented for mobile devices.

6.2.3 MAS accepts the respondents' feedback and has revised the guidance for clarity.

6.3 **Voiding Hardware Tokens, Passwords and PINs after 3 Months / Increasing Strength of Customers' PINs (paragraphs F.2.2 and F.3.3)**

6.3.1 One respondent proposed that FIs implement controls to void hardware tokens, passwords or PINs if customers do not use them within 3 months of issuance.

6.3.2 Another respondent highlighted that implementing dual controls for online account activation will not be necessary as dual control is already implemented through password generation and PIN mailer printing.

MAS' Response

6.3.3 The Guidelines provide guidance on the key IT controls, processes and procedures that FIs should implement to ensure the security of online financial systems. FIs should take a holistic approach in determining the adequacy of controls that are already in place in its environment and implement security measures that are commensurate with the risks.

6.4 **Non-Hardware Tokens (paragraph F.2.2(h))**

6.4.1 Some respondents asked whether FIs can use non-hardware tokens instead of hardware tokens.

MAS' Response

6.4.2 The guideline in paragraph F.2.2(h) is for hardware tokens. FIs should implement strong mechanisms for two-factor authentication, which include non-hardware tokens. FIs should perform a thorough risk assessment of the strength of the two-factor authentication solution before implementing it.

6.5 **Customer Education (section F.3)**

6.5.1 One respondent suggested that customer education be conducted at an industry-wide level, rather than at the individual FI level. Another respondent suggested that customer education be extended to third-party vendors as well. It was also highlighted that providing customer education for every customer places an unnecessary financial burden on the FI.

MAS' Response

6.5.2 MAS notes the feedback. FIs may wish to conduct consumer education programmes through their respective associations.

6.5.3 However, FIs should provide sufficient information to their customers on the risks associated with online services that are unique to their business and not covered by a generic industry-wide education programme. Where relevant, vendors should be made aware of the FIs' security policies and standards.

6.6 **Application Session Termination and Clearing of Browser Cache (paragraph F.3.4)**

6.6.1 One respondent commented that as a best practice, customers should terminate their mobile application session, and clear their browser cache after usage.

MAS' Response

6.6.2 The advice to customers to terminate a mobile application session is stated in paragraph F.3.4(f), "Log off the online session". MAS agrees with the respondent's feedback and has included a statement on the clearing of the browser cache into the Guidelines.

7 **Others**

7.1 **Chapters 1 and 2 - Introduction and Application of The Guidelines**

7.1.1 **Applicability of Guidelines, Regulations, Circulars and Notices (paragraphs 2.0.1 and 2.0.2)**

7.1.1.1 Several respondents highlighted that not all aspects of MAS' existing guidelines and circulars have been included in the Guidelines. Some respondents asked whether the Guidelines will supersede MAS' Guidelines on Outsourcing or MAS Circular No. SRD TR01/2011. Other respondents asked whether the Notice supersedes other notices issued by MAS.

MAS' Response

7.1.1.2 The Guidelines do not replace or supersede the Guidelines on Outsourcing and the circular on IT Outsourcing. However, the following guidelines, circulars and security advisories will be cancelled upon the issuance of the Guidelines and Notice:

a. Internet Banking and Technology Risk Management Guidelines June 2008;
b. SRD Cir TR02/2010, Information Reliability, Resiliency and Recoverability;
c. SRD Cir TR02/2009, Technology Risk Management;
d. SRD Cir TR01/2009, End-Point Security and Data Protection;
e. SRD Cir 02/2005, Two-Factor Authentication for Internet Banking;
f. Spyware, April 2004;
g. Phishing, November 2003;
h. Internet Kiosk, September 2003;
i. Wireless Local Area Network, December 2002;
j. Internet Banking PIN Verification, April 2002;
k. Internet Banking Security Responsibility, November 2001; and
l. Internet Banking Network Security, July 2001.

7.1.2 **MAS' Definition of Financial Institutions and Applicability of Guidelines on Systems hosted Overseas (paragraphs 1.0.1 and 2.0.1)**

7.1.2.1 Several respondents asked how MAS defines "Financial Institutions" and whether the Guidelines apply to FIs that operate systems which are hosted in overseas subsidiaries or branch offices.

MAS' Response

7.1.2.2 In the Guidelines, the definition of "Financial Institution" carries the same meaning as what is provided in section 27A(6) of the Monetary Authority of Singapore Act.

7.1.2.3 Outsourcing by FIs, in any configuration or at any location should not impede MAS in carrying out its supervisory functions. In this regard, guidelines, circulars, notices, regulations and Acts governed by MAS are applicable to FIs, which operate systems that are used by Singapore operations but hosted overseas.

7.2 **Chapter 3 - Oversight of Technology Risks by Board of Directors and Senior Management**

7.2.1 **Involvement of Board of Directors and Senior Management in Technology Risk Management (section 3.1)**

7.2.1.1 Several respondents expressed concerns over MAS' expectation that both the board of directors and senior management are responsible for implementing

internal controls and risk management practices in FIs. Some respondents commented that foreign-incorporated entities often delegate the responsibility for technology risk management to local management. Other respondents asked whether the involvement of the board of directors and senior management in providing management oversight is sufficient to meet regulatory expectation.

MAS' Response

7.2.1.2 We note the respondents' concerns. The board of directors and senior management of a FI are ultimately responsible for the technology risks assumed by the FI and the manner in which these risks are managed. In this regard, the board of directors should review and approve the strategies and policies related to the management of technology risks in FIs, and ensure that senior management manages technology risk effectively.

7.2.2 **Employee Screening Process (paragraph 3.3.1)**

7.2.2.1 Many respondents asked that clarity be provided on MAS' expectation that all FIs should implement a comprehensive and effective employee screening process. Some respondents also asked whether the term "employee" will include contractors or vendors.

MAS' Response

7.2.2.2 A comprehensive and effective employee screening process seeks to ensure that each FI is appropriately staffed at all levels by qualified persons at the point of their recruitment, as well as on an on-going basis. The frequency and scope of screening should take into account the criticality of a position. In this regard, each FI should determine the appropriate checks and verifications necessary to screen employees effectively, especially for staff handling critical IT functions.

7.2.2.3 The use of contract employees, contractors or vendors should not result in a weakening of internal controls in the FI. In this regard, each FI should ensure that an adequate screening process is in place for such persons serving the institution, and that it has appropriate safeguards to manage any potential risks arising from the employment of or outsourcing to such persons.

7.2.3 **IT Security Awareness Training for Contractors and Vendors (paragraph 3.4.2)**

7.2.3.1 Some respondents expressed concerns over MAS' expectation that FIs conduct IT security awareness training for their service providers. A few respondents commented that it may not be cost-effective for FIs to do so, especially for short-term outsourcing engagements. Other respondents suggested that FIs should ensure

that their service providers had undergone IT security awareness training prior to engaging them.

MAS' Response

7.2.3.2 FIs should ensure that vendors and contractors engaged to work at or for the FIs understand relevant IT security policies at the FI, even if these vendors and contractors have undergone IT security awareness training at their companies.

7.3 Chapter 4 - Technology Risk Management Framework

7.3.1 Technology Risks Assessment (paragraph 4.0.2(e))

7.3.1.1 Several respondents asked MAS to provide explicit guidance on how often FIs should update and monitor technology risk assessments. One respondent highlighted that risk should be a function of impact and likelihood. Another respondent commented that non-quantifiable risks should be considered during risk assessments as well.

MAS' Response

7.3.1.2 MAS does not intend to mandate the frequency at which FIs should update or monitor their technology risk assessments. MAS expects FIs to establish a process to assess and determine the appropriate frequency for conducting such reviews to ensure that their IT policies, standards, guidelines, and procedures remain relevant to their operating environment.

7.3.1.3 MAS agrees with the respondents that risk should be a function of impact and likelihood, and that non-quantifiable risk should be considered during risk assessments as well. These suggestions have been incorporated into the Guidelines.

7.4 Chapter 5 - Management of IT Outsourcing Risks

7.4.1 Inclusion of Paragraphs in Outsourcing Contracts to Facilitate Regulatory Supervision (paragraph 5.1.3)

7.4.1.1 Several respondents expressed concerns over MAS' expectation for FIs to include explicit paragraphs in outsourcing contracts to facilitate regulatory supervision. Some respondents highlighted that not all FIs will have the legal prerogative to meet this expectation. Other respondents sought clarification on the applicability of this expectation on overseas service providers and legacy outsourcing arrangements.

MAS' Response

7.4.1.2 MAS notes the respondents' concerns. The objective of the paragraph is to ensure that sound and robust practices are implemented by FIs for outsourced IT services and systems. Outsourcing by FIs in any configuration or at any location should not impede MAS in carrying out its supervisory functions. The right to examine service providers to obtain information stored at, or processed by service providers, and the right to access any report or finding made on the services rendered to FIs is integral to MAS' supervisory efforts.

7.4.1.3 MAS agrees with the respondents that FIs may not have the legal prerogative to amend legacy outsourcing contracts. In this regard, MAS expects FIs to ensure that the expectation is met when revising, renewing or extending legacy outsourcing agreements.

7.4.2 **DC On-Site Visit (paragraph 5.1.14)**

7.4.2.1 Several respondents asked whether internal staff can perform on-site DC visits at the service provider's premises. Other respondents asked MAS to provide explicit guidance on how often an on-site DC visit should be performed. One respondent proposed that on-site DC visits be performed only when there are significant changes to the risk profile of DCs. Another respondent suggested that periodic penetrating testing be performed only when DCs are hosting critical systems or data.

MAS' Response

7.4.2.2 Outsourcing in any form or at any location should not result in a weakening of internal controls in FIs. In this regard, the responsibilities for effective due diligence, oversight and management of outsourcing, as well as accountability for all outsourcing decisions, continue to rest with FIs, its board and senior management. FIs should ensure that on-site DC visits be performed by qualified personnel, at a frequency that is commensurate with their level of risk exposure.

7.4.2.3 This paragraph has been removed from Chapter 5 as the subject is covered under Chapter 10 – Data Centres Protection and Controls.

7.4.3 **Cloud Computing Due Diligence (section 5.2)**

7.4.3.1 Several respondents requested that more guidance be provided on the types of due diligence FIs will be expected to perform when engaging cloud computing service providers. Some respondents also asked whether MAS will be releasing any guidelines on cloud computing.

MAS' Response

7.4.3.2 As cloud computing is a form of outsourcing, the guidance in the Guidelines would apply. In this regard, all FIs are expected to perform risk assessments and the necessary due diligence before engaging in any IT outsourcing arrangements, including use of cloud computing. FIs should also ensure compliance with relevant regulations and notices, as well as meet expectations articulated in circulars and guidelines issued by MAS.

7.5 **Chapter 6 - Acquisition and Development of Information Systems**

7.5.1 **Establishment of Separate Physical or Logical IT Environments (paragraph 6.2.5)**

7.5.1.1 Some respondents noted that the expectation to set up separate physical or logical environments for unit, integration, system and user acceptance testing (UAT) may be overwhelming for small-scale FIs.

MAS' Response

7.5.1.2 The Guidelines are aligned with industry best practices. The FI should perform an assessment of the setup of its test environment relative to its operations, and implement appropriate controls over the different environments.

7.5.2 **Source Code Review (section 6.3)**

7.5.2.1 Some respondents noted that source code reviews may not be feasible for off-the-shelf software as FIs do not have access to the source code.

MAS' Response

7.5.2.2 MAS recognises that FIs may not have access to proprietary source codes for software developed by vendors. As part of FIs' due diligence and in order to obtain assurance that the source code is secure, FIs should obtain an undertaking from the software vendor to confirm that independent source code review is performed or conduct additional testing prior to the release of software developed by vendors.

7.5.3 **End User Development (section 6.4)**

7.5.3.1 Some respondents noted that the End User Developed Applications (EUDAs) stated in the consultation paper applied to all EUDAs. The respondents suggested that the scope defined to include only EUDAs determined by FIs to be business critical.

MAS' Response

7.5.3.2 MAS accepts the respondents' suggestion and has revised the Guidelines such that FIs are expected to assess the criticality of EUDAs and implement the appropriate processes and controls to secure EUDAs.

7.6 Chapter 7 - IT Service Management

7.6.1 Connection to the internet (paragraph 7.2.2)

7.6.1.1 Many respondents commented that the expectation that only the production environment is allowed to connect to the internet may not be feasible as other environments may also need to connect to the internet for work-related purposes.

MAS' Response

7.6.1.2 MAS agrees with the respondents' feedback. As controls in the non-production environment may be different or less stringent than those in the production environment, FIs are expected to assess the risks and implement sufficient controls before connecting a non-production environment to the internet. MAS has revised the Guidelines on this subject.

7.6.2 Incident Reporting Timeframe (paragraph 7.3.8)

7.6.2.1 Many respondents enquired on the type of incidents that should be reported to MAS within the 30 minutes timeframe.

MAS' Response

7.6.2.2 Any IT security incident or system malfunction that has severe and widespread impact on an FI's operations, or materially impacts the FI's service to its customer is a reportable event. An FI should notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a Relevant Incident as defined in the Notice.

7.6.2.3 To avoid duplication with the Notice on Technology Risk Management which will be issued together with the Guidelines, the reporting timeframe has been removed from the Guidelines.

7.6.3 Incident Investigation and Disclosure (paragraphs 7.3.9, 7.3.10 and 7.3.12)

7.6.3.1 Some respondents enquired about the format for public disclosure of IT incidents.

7.6.3.2 In addition, the respondents suggested that the 1 month timeframe to submit the incident root-cause report should be defined only for critical applications.

MAS' Response

7.6.3.3 MAS will leave it to the discretion of the FIs on the format for public disclosure of IT incidents as it depends on the specific circumstances at that time of the incident such as if there is an ongoing investigation by the authorities.

7.6.3.4 To avoid duplication with the Notice, the timeframe for submitting the incident root-cause report has been removed from the Guidelines.

7.7 Chapter 8 - Systems Reliability, Availability and Recoverability

7.7.1 Definition of Near Zero Downtime (paragraph 8.1.3)

7.7.1.1 Some respondents enquired on the definition of near zero downtime stated in the Guidelines.

MAS' Response

7.7.1.2 The Guidelines is not meant to be prescriptive. It expresses best practices and encourages the FI to implement an IT infrastructure which can support high availability for its critical systems. MAS has revised the Guidelines accordingly.

7.7.2 Active-Active Environment (footnote 9)

7.7.2.1 Some respondents commented that the expectation on establishing an active-active environment may be overly prescriptive and suggested to allow FIs to determine the appropriate setup to achieve near-zero downtime.

MAS' Response

7.7.2.2 MAS accepts the respondents' suggestion that FIs can deploy other solutions to achieve high availability, and has revised the Guidelines accordingly.

7.7.3 Disaster Recovery Test Frequency (paragraph 8.3.2)

7.7.3.1 Some respondents suggested that the disaster recovery test frequency should be based on the criticality of the applications and not fixed at an annual cycle.

MAS' Response

7.7.3.2 IT disaster recovery testing is important as it enables the FI to ensure that systems are recoverable in the disaster recovery environment, rehearse procedures for activating the IT disaster recovery plan, test the notification process for key personnel involved in the recovery, and verify that recovery procedures for different disaster scenarios are effective. Hence, it is important that FIs test the IT disaster recovery plans at least annually.

7.8 Chapter 9 - Operational Infrastructure Security Management

7.8.1 Data Loss Prevention (section 9.1)

7.8.1.1 Many respondents enquired about the endpoint devices, communication channels and the type of data that should be protected as well as the method of protection.

MAS' Response

7.8.1.2 MAS does not prescribe methods that FIs should use to protect confidential information. FIs are expected to conduct risk assessments to determine the appropriate data loss prevention strategy to ensure adequate protection over confidential and sensitive information.

7.8.2 Internal Network Protection (paragraph 9.3.4)

7.8.2.1 Respondents noted the need for security measures on internal networks. The respondents enquired whether components other than the firewall, which is stated in the Guidelines, can be deployed so long as similar effectiveness is achieved.

MAS' Response

7.8.2.2 MAS agrees with the respondents' suggestion to allow the deployment of other security components that are as effective as firewalls in protecting the internal network and minimising the impact of security exposures originating from third party or overseas systems. MAS has revised the Guidelines accordingly.

7.8.3 Frequency of Security Testing (paragraph 9.4.1)

7.8.3.1 Respondents noted the need to conduct adequate security testing such as penetration testing and vulnerability assessment. The respondents suggested that the quarterly cycle for vulnerability assessment should be defined for critical applications only.

MAS' Response

7.8.3.2 MAS agrees with the feedback and has removed the guidance on "quarterly cycle" from the paragraph in the Guidelines. FIs are expected to conduct risk assessments to determine the frequency of vulnerability assessments to be conducted.

7.8.4 Security Monitoring (section 9.6)

7.8.4.1 Many respondents enquired about the scope of security monitoring, the tools to use as well as the review timeframe.

MAS' Response

7.8.4.2 MAS does not prescribe the scope and approach for security monitoring. As FIs vary in size and complexity of operations, each FI is expected to conduct its risk assessment to determine the scope and approach for security monitoring.

7.9 Chapter 11 - Access Control

7.9.1 Enforcement of Segregation of Duties Principle and Two-Factor Authentication for Privileged Users (paragraphs 11.0.1(b) and 11.2.3(a))

7.9.1.1 Many respondents commented that not all FIs will have the resources to enforce segregation of duties for all critical IT functions. Several respondents also commented that it will be too onerous for FIs to implement two-factor authentication for all privileged users and requested that leeway be granted to FIs that had controls in place to detect and prevent fraud or error.

MAS' Response

7.9.1.2 MAS notes the respondents' feedback. Each FI is expected to ensure that its control framework is adequate and commensurate with its operations.

7.9.1.3 Two-factor authentication is one of the security measures to manage privileged user IDs. In this regard, FIs can implement other strong controls as long as they can meet the objectives of these Guidelines.

7.10 Chapter 12 Online Financial Services

7.10.1 Scope of Online Financial Services and Two-Factor Authentication (paragraph 12.1.7)

7.10.1.1 Some respondents asked about the scope of "online financial services", and of FIs, services, systems and transactions, which require the implementation of two-factor authentication. One respondent also suggested refining the scope to distinguish between the different kinds of online services relating to payments versus trading-based transactions.

7.10.1.2 One respondent suggested that two-factor authentication should only be required for login of internet-facing systems instead of all systems providing online financial services.

7.10.1.3 Another respondent suggested waiving the need to implement two-factor authentication to authorise transactions for online financial systems servicing institutional investors, accredited investors or corporate entities (both offshore and locally incorporated).

MAS' Response

7.10.1.4 'Online financial services' refers to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices.

7.10.1.5 Although trading applications will not affect the customers' bank account directly, the risks such as reputational damage to the FI and possible market manipulation through stolen online trading accounts should be considered. MAS' view is that distinction between payment and trading-based transactions is not required.

7.10.1.6 Two-factor authentication should be implemented for login to internet-facing systems. In addition, FIs are expected to implement two-factor authentication for other online financial services where strong authentication can reduce the risk of identity theft.

7.10.1.7 Transaction signing is required for high-risk transactions. As defined in paragraph E.2.2(b) of the Guidelines, high risk transactions include changes to sensitive customer data (e.g. customer office and home addresses, email addresses and telephone contact details), registration of third party payee details and revision of funds transfer limits.

7.10.1.8 MAS notes the respondents' feedback that there are other controls which can be implemented for authorising transactions for online financial systems servicing institutional investors, accredited investors or corporate entities (both offshore and locally incorporated). The Guidelines has been updated to reflect that FIs should perform a risk assessment of alternate systems and ensure that the level of security of controls for authorising the transactions are similar to or better than transaction-signing mechanisms.

7.10.2 **Online Financial Services Security (paragraphs 12.1.3, 12.1.5, 12.1.8)**

7.10.2.1 One respondent suggested that implementation of cryptography technology that had been evaluated by reputable vendors or authoritative professional bodies may not be adequate as the assessment conducted by the verifying entity may be subjected to contention.

7.10.2.2 Several respondents also enquired about MAS' definition of "erratic system activity", as well as how it can be detected.

7.10.2.3 A respondent suggested that security measures used for combating man-in-the-middle attack (MITMA) should only be implemented for high-risk transactions.

MAS' Response

7.10.2.4 MAS agrees that cryptography technology that is evaluated by different reputable parties can be subjected to contention. Hence, the FI should exercise judgment when reviewing the assessment provided by the external parties and address any concerns before implementing any encryption solution.

7.10.2.5 Erratic or abnormal system activity refers to a system event or a series of system events that deviate(s) from the usual system behaviour or usage pattern captured by the FI's system monitoring tools or documented by the FI's daily / weekly logs.

7.10.2.6 MITMA refers to a scenario where an interloper is able to read, insert and modify at will, messages between two communicating parties without either one knowing that the link between them has been compromised. FIs should carry out an assessment on the risks and customer usage experience in assessing whether to implement security measures to counter MITMA for non-high risk transactions.

7.11 Chapter 14 - IT Audit

7.11.1 Applicability of Guidelines on External Audit Function and Wide-Ranging IT Audit Scope (Chapter 14)

7.11.1.1 One respondent asked if expectations in this chapter of the Guidelines apply to the external audit function of FIs. Another respondent asked what constitutes MAS' expectation of an IT audit scope that is "wide-ranging".

MAS' Response

7.11.1.2 This chapter in the Guidelines is applicable only to the IT internal audit function in FIs for providing the board of directors and senior management with an independent and objective assessment of the effectiveness of internal control systems.

7.11.1.3 A comprehensive IT audit scope should cover all IT functions and processes supporting the business operations of an FI in Singapore.

7.11.2 Updating IT Audit Committee on Changes to IT Audit Plan (paragraph 14.1.4)

7.11.2.1 Several respondents commented that it will be too onerous for each FI to keep its IT Audit Committee apprised of every change to the IT audit plan. Some respondents suggested that the IT Audit Committee be notified of significant changes to the IT audit plan instead.

MAS' Response

7.11.2.2 MAS has considered the respondents' suggestion and has removed the guidance from the Guidelines.

7.12 **Appendix A - Systems Security Testing and Source Code Review**

7.12.1 **Incorporating Source Code Review into System Development Life Cycle ("SDLC") (paragraph A.1.1)**

7.12.1.1 Many respondents commented that it may not be cost-effective for FIs to perform source code reviews for all systems, especially for small-scale development projects. One respondent suggested that vulnerability assessments or penetration testing be performed in place of source code reviews. Another respondent suggested that source code reviews be limited to those for critical systems.

MAS' Response

7.12.1.2 Systematic examination of computer source code is integral to FIs' efforts in mitigating security threats and weaknesses from their systems. The objective of including source code review as part of SDLC is to identify malformed programs or malicious codes which are not detectable from system testing, vulnerability assessments, vulnerability scans or penetration tests. MAS expects FIs to put in place a framework to determine the depth and scope of source code reviews for their systems.

7.12.2 **Preventing Security Defects through Logging (paragraph A.1.3(c))**

7.12.2.1 Several respondents highlighted that logging will not intrinsically prevent security defects and asked that MAS provides more guidance on this expectation.

MAS' Response

7.12.2.2 MAS accepts the respondents' suggestion and has revised the Guidelines.

7.13 **Appendix B - Storage System Resiliency**

7.13.1 **Storage Systems Architecture and Connectivity Review (paragraph B.2.1)**

7.13.1.1 Some respondents requested MAS to reconsider the paragraph for regular reviews of the architecture and connectivity of storage systems and suggested instead that the reviews should be conducted during the design stage of the implementation and prior to changes made to the infrastructure.

MAS' Response

7.13.1.2 To ensure the resiliency, availability and recoverability of the FIs' storage systems, they should determine the frequency of reviews on the architecture and connectivity of its storage systems, and it should not be limited to the design stage of implementation nor before changes made to the infrastructure.

7.14 **Appendix C - Cryptography**

7.14.1 **Hardware Security Module (paragraph C.3.3)**

7.14.1.1 Two respondents enquired whether the use of hardware security module for storing all encryption keys is mandatory.

MAS' Response

7.14.1.2 For the protection of sensitive and critical data, tamper resistant devices such as hardware security modules should be used to store all encryption keys.

7.15 **Appendix D - DDoS Protection**

7.15.1 **Protection against Distributed Denial of Service (DDoS) attacks (Appendix D)**

7.15.1.1 A few respondents have commented that a new class of Distributed Denial of Service (DDoS) attacks has emerged that focuses on layer 4 through layer 7 of the protocol stack and hence, suggested that the need for FIs to implement DDoS protection mechanisms that actively guards against such attacks be included in the Guidelines.

MAS' Response

7.15.1.2 MAS does not prescribe solutions to FIs on protection against different types of DDoS attacks. FIs are expected to perform risk assessments to determine the appropriate protection measures needed to counter various forms of DDoS attacks.