4 October 2021

To:
Yeow Seng Tan
Executive Director
Technology and Cyber Risk Supervision Department
Monetary Authority of Singapore

ASIFMA response to MAS FINSTAR consultation

Dear Yeow Seng,

ASIFMA appreciates the opportunity to respond to MAS' consultation on *the Draft Financial Sector Cyber Threat Alert & Readiness ("FINSTAR") Framework*. We also very much appreciate the extension of the response deadline by one week to 4 October. Financial institutions are reliant on interrelated computer systems, and continue to be targeted in cybersecurity attacks. As such, our members recognize the importance of timely detection of significant cybersecurity threats, and fully support the MAS' goal of sensitising FIs to the prevailing sectoral cyber threat level of the Singapore financial sector and to raise the overall effectiveness of FIs' cyber defenses.

ASIFMA members very much support threat intelligence sharing as a key pillar in their cyber resilience programs. We therefore welcome any additional sharing of information that MAS has gathered from various resources, particularly threat intelligence obtained from cyber incidents reported by FIs, and believe this will provide additional value and insights into to the threat landscape. We submit however that this threat intelligence provided by MAS is an additional contributing factor that can augment and complement existing programs that our members already have in place and should not be linked to prescriptive cybersecurity measures that FIs need to adopt. FIs in Singapore are already subject to the MAS Technology Risk Management Guidelines and the Cyber Hygiene Notice, which already have requirements around threat detection, vulnerability management and incident response.

We therefore believe change is warranted in several areas of the draft FINSTAR framework, and in what follows, we propose revisions in those areas. We are grateful for your consideration and hope these can be reflected in the final framework.

Legal weight

We note that the draft is a "framework" and that Table 2 in the draft framework refers to readiness "guidelines". Our members would like to understand to what extent the Framework will be legally binding or whether the Framework represents suggestions/good practices for FIs to implement. We understand from email conversations with the MAS that the FINSTAR framework and readiness guidelines are not legally binding requirements but that the objective of FINSTAR Alert Levels is to better contextualise existing MAS Cyber Threat Alerts and provide a framework for MAS to communicate the cyber threat level for Singapore's

financial sector. We suggest that it is further clarified and confirmed in the final framework that the framework and the readiness guidelines are guidelines/suggestions that are not legally binding.

If members have a robust framework that receives and processes similar threat alerts, commensurate with what is advised in the consultation paper, they should be able to rely on these internal processes and not have to establish separate/stand-alone processes to meet the proposed Framework. FIs should be allowed to conduct an internal assessment whether their alert monitoring mechanism is sufficient to handle various threat levels, without requiring further action based on each threat notification.

We would also be grateful if the MAS could outline if and how they are planning to assess FIs' implementation of the framework during its supervisory assessments.

No one-size fits all

For firms that have a well-established cyber resilience programs, actual responses to cyber threats should be driven by firm-defined triggers. This is because depending on a firm-specific context (e.g. how and to what extent a certain system is used), what is a high threat for one firm could merely be a low threat for another firm. Internal, firm-specific circumstances will need to be taken into account for FIs to define their responses and the one-size-fits-all approach that the draft FINSTAR framework seems to be suggesting is counter-productive and could lead to significant operational disruptions for FIs.

We encourage the MAS to take a flexible and principle-based approach instead of mandating specific actions following MAS's alert level. We suggest the MAS should recognize FI's own threat analysis process and risk assessment, which will sufficiently cover Singapore and the alerts shared by MAS. Having Singapore-specific processes and timelines adds to international firms' administrative burden draining cyber defense resources without adding much value and can create practical implementation issues where global systems are in use.

Results of risk assessment

It will be good to understand how the results of a firms' risk assessment following a FINSTAR alert impacts that firm's suggested response. For example:

- After the issuance of a FINSTAR alert, if a firm's impact assessment demonstrates that the firm is not or not significantly impacted, does the firm need to stay on "red alert" level?
- How does the risk assessment change the response? E.g. after the issuance of an orange or red alert, a firms determines that they have vulnerable devices but considers they have existing appropriate mitigating controls. Do firms still have to remove remote access?

Need for calibration

Our members suggest there is a need to further calibrate the threat levels and submit that the "Yellow" level is close to BAU. The Yellow Alert level will require significant work for a threat that may have little impact to

our members' operations over 72 hours. There also seems to be no significant difference in response between Orange and Red other than for Connectivity Management.

If not done so yet, we suggest a retrospective analysis be conducted to assess how many times the levels will have been triggered in the last 2 years for the different incidents and the respective rationales as this will help to calibrate the framework. If there were no ORANGE and RED alerts in the past 2 years, we will be grateful if the MAS could provide the most recent examples of incidents falling under each respective category. We would appreciate it if the analysis results can be shared with our members.

We also submit that it should be clear what triggered a certain alert level and that clear intelligence is provided by the MAS on specifically which technology and/or systems are being targeted and how.

Definition of critical systems

The draft framework makes multiple references to 'critical systems'. We kindly ask the MAS to clarify what is the definition of 'critical systems' and whether it is the same definition as in MAS Notice 644 on Technology Risk Management.

Timelines

We submit that the timeframes to complete risk and impact assessment (i.e. 24 hours for RED, 48 hours for ORANGE and 72 hours for YELLOW) are tight and we would like to better understand what are the expectations. We would also like to reiterate that it is critical for the MAS to take a flexible and outcome-focused approach, and allow global FIs to leverage their existing threat intelligence program and refrain from prescribing timelines and Singapore specific processes.

Implementation questions

- We submit that some of the readiness guidelines for the RED alert (e.g. disabling external connections) are far-reaching and can put firms at risk. Shutting off global systems just for Singapore is challenging and is a far-reaching decision that should be taken by the FI and not by the regulator. E.g. if the MAS were to mandate firms to shut down a certain trading system, this could lead to failed trades and adverse customer impacts against which firms are not legally protected. The potential legal consequences must be considered if actions are mandated. As highlighted above, we submit that firm response actions should be driven by their existing processes.
- We would like to better understand how the information feed will flow so as to ensure the CISOs are instantly informed, particularly in light of the currently proposed risk assessment timelines. If the information will be provided via MASNET, it will take some time for the info to reach the CISOs as for most firms, it is the Compliance team that is signed up for MASNET who would then need to further circulate the alerts internally. To ensure alerts are received by stakeholders in a timely manner, notifications should directly reach the key roles identified per the MAS Guidelines on Individual Accountability and Conduct – namely the CIO/CTO/Head of IT and the CISO/Head of Information Security. Alternately the MAS can have a permissioned subscription service to which authorized

individuals from the members can be added. This will ensure that those who need to respond to the alerts receive them in a timely manner without having to wait for it to be retrieved from the MASNET system. We would also like to clarify if FINSTAR is to replace any of the existing notifications, e.g. FINTEL notifications.

Additional specific comments for each of the threat levels can be find in the last column of the below table:

	Yellow	Orange	Red	Comments
Identify	**Risk & Impact Assessment** • Perform risk and impact assessment on the identified cyber threat.	**Risk & Impact Assessment** • Determine the critical systems which are susceptible to the identified cyber threat.		
	Identify Implications • Inform relevant key internal stakeholders, system owners and decision makers about the identified cyber threat to assess the possible implications.			
Protect		**Connectivity Management** • Remote access to identified critical systems should be blocked except for the purposes of mission critical activities, security patching or incident response.	**Connectivity Management** • Disable external connections that are not required for mission critical activities based on the risk and impact	Orange – It may not be practical to block all activities. Orange and Red – what is the definition of mission critical activities?
		Identity & Access Management • Restrict all privileged accounts access of identified critical systems to only		This may not be practical to apply given FIs may have

		mission critical activities, security patching or incident response.	to significantly modify accounts that are used at infrastructure levels.
		Change Management • Limit system changes only to security patching required to address the identified cyber threat.	This may not be practical to employ. This implies FIs are only doing patching to address the threat and not any other patching. At the same time FIs are effectively freezing business progress potentially not just for Singapore but other nations.
	Vulnerability & Patch Management • Scan and check if the IT environment contain the identified vulnerabilities. Obtain latest patches and prioritise patching based on threat intel received. • Test and install patches as soon as possible. (If patching is not possible, to implement compensating controls including increasing monitoring of the vulnerable systems.)		
Detect	**Security Monitoring** • Inform security operations or outsourced vendors to be on heightened alert and focus on the	**Security Monitoring** • Step-up security operations or outsourced vendors to expand monitoring and coverage.	Orange/Red - "Step-up" what practical change is expected and how does it differ to Respond?

	indicators of attack/compromise identified cyber threat.		
Respond	**Incident Response** • Incident response personnel should be on heightened alert and monitor updates on the identified cyber threat.	**Incident Response** • Place cyber incident response team (and retainer service if applicable) on hot standby.	
	Situation Update • Provide regular updates on new developments in the cyber threat situation to key internal stakeholders, system owners and decision makers.		
Recover	**Business Continuity Planning (BCP) & Disaster Recovery (DR)** • Put the BCP and DR teams on hot standby and activate them in the event of disruption.		

Also, some of the examples in the draft Framework seem to focus on attacks against Singapore FIs. The MAS might want to consider expanding the Framework to include key suppliers. If there is a compromise on suppliers (non-FIs) that could impact FIs – this level of threat intelligence from the MAS (if available) will be helpful.

Need for international harmonisation

We appreciate the MAS' sharing of threat intelligence, particularly those gathered through FI incident reporting. Incident reporting could enable financial regulators to assess the severity of cyber-threats, compare situations and understand trends and identify systematic implications, which can be very helpful in providing additional insights to an FI's current threat intelligence program. To enable a financial regulator's capability of gathering intelligence through incident reporting, it is critical for financial regulators to address fragmented reporting requirements including varying definitions, reporting thresholds, and timelines all of which could

diminish a financial regulator's capacity to conduct proper analysis. Fragmented reporting requirements create immense operational burden and confusion leading to a weakened cybersecurity posture for the entire financial sector. Additionally, prescriptive reporting requirements that do not take into account an FI's particular business or risk profile can unintentionally inhibit strong cybersecurity by making it more difficult to identify and address the most important incidents. Fragmented reporting timelines and jurisdiction-specific prescriptive processes can often create operational confusion amongst large global firms, and slow down the process of timely reporting.

We encourage MAS to work with regulators globally to develop a standardized framework and taxonomy to reach a common understanding of a situation and we are supportive of the work of the Financial Stability Board on that front.

Of note is that the MAS suggested alert framework is different from the US Financial and Banking Information Infrastructure Committee (FBIIC) All-Hazards Incident Response Plan (FBIIC-IRP) severity scheme (in Annex), and we would urge the MAS to work towards international alignment and standardization as opposed to introducing a new, prescriptive framework for the Singapore market.

We are grateful for the opportunity to share our feedback on the proposed FINSTAR framework and appreciate MAS's extention of deadline. The financial industry is keen to engage with the MAS on important topics on technology and cybersecurity and encourage the MAS to adopt 1 month response time for future consultations to allow for in-depth discussions and comprehsive responses from the sector globally. We hope our suggestions will be reflected in the final framework andare more than willing to discuss our response in more detail during a meeting and remain at your disposal for any questions you might have in relation to the above response.

Best regards

Laurence Van der Loo

Executive Director Technology and Operations

ASIFMA

Annex: *US* Financial and Banking Information Infrastructure Committee (FBIIC) All-Hazards Incident Response Plan (FBIIC-IRP) severity scheme

Significant Incidents An incident or series of incidents likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.	**Emergency Level 5**	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.	An incident or series of incidents, *poses an active or imminent threat* of sector-wide outage(s) and/or catastrophically destructive compromise to sector National Critical Functions, with nearly certain likelihood of catastrophic damage resulting in a potential collapse of the capital markets, payment, clearing, or settlement services, or nationwide loss of confidence in the financial system.
	Severe Level 4	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	An incident or series of incidents, *likely to result in sector-wide outage(s) or significant destructive compromise* to sector National Critical Functions, with at least roughly even odds to lead to significant adverse impact to capital markets, payment, clearing, or settlement services for a majority of financial institutions with associated impact to consumer confidence.
	High Level 3	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	*Likely to result in demonstrable* and observable negative or adverse impact to critical operations of National Critical Functions, or at least roughly even odds of isolated run(s) on the banks by personal or corporate bank customers or the possibility of a regional/national disruption to capital markets, payment, clearing, or settlement services. Consumer confidence directly impacted by an incident that compromises day-to-day banking or financial operations.
Incidents An event that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, or physical or virtual infrastructure.	**Medium Level 2**	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	*May impact* and disrupt financial services operations. For a cyber-incident, likely damage or disruption to critical operations at a single institution, or non-critical operations at several financial institutions, or compromise of several firm's confidential data with potential to be mitigated quickly. For a physical event, disruptions or impacts to banking or financial facilities in addition to local physical infrastructure, including main thoroughfares or roads that limit access to banking or financial facilities.
	Low Level 1	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	*Unlikely to impact* financial services operations and indicates localized, contained compromise or disruption of a U.S. financial institution. For a cyber-incident, no exploits have been identified, or exploits have been identified but no significant damage, disruption or system compromise has occurred. For a physical event, localized disruptions or impacts to banking or facilities.
	Baseline Level 0	Unsubstantiated or inconsequential event.	Unsubstantiated or inconsequential event.