

By E-mail (csa_cs_bill_feedback@csa.gov.sg)

Cyber Security Agency of Singapore
5 Maxwell Road
#03-00 Tower Block, MND Complex
Singapore 069110

Your reference:
Our reference: LNG/CLJ
Direct Dial: +65 6410 2215 / 6506 2752
E-mail: lana.ng@cliffordchance.com
lijun.chui@cliffordchance.com

24 August 2017

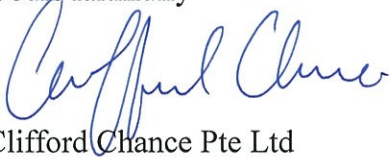
Dear Sirs

Public Consultation for the Cybersecurity Bill

1. We enclose herewith our response to the MCI/CSA Consultation Paper on the draft Cybersecurity Bill, prepared and submitted in collaboration with ASIFMA (Asia Securities Industry & Financial Markets Association), FIA (Futures Industry Association) and ISDA (International Swaps and Derivatives Association) and its members.
2. We welcome the holistic approach proposed for the draft Cybersecurity Bill. Our response focuses on services relating to derivatives trading, clearing and settlement.
3. We look forward to further opportunities to discuss sector-specific issues as we move forward in this consultation process. In the meantime, if you have any questions, please do not hesitate to contact:
 - a. **Clifford Chance:** Lena Ng, Partner, Clifford Chance Pte Ltd at lana.ng@cliffordchance.com or +65 6410 2215; Chui Lijun, Senior Associate, Clifford Chance Pte Ltd at lijun.chui@cliffordchance.com or +65 6506 2752.
 - b. **ASIFMA:** Wayne Arnold, Executive Director, Head of Policy and Regulatory Affairs, Asia Securities Industry & Financial Markets Association (ASIFMA) at warnold@asifma.org or +852 8531 6560.
 - c. **FIA:** Phuong Trinh, Vice President of Legal & Policy, Asia-Pacific, Futures Industry Association at ptrinh@fiaasia.org or +65 6549 7335.

- d. **ISDA:** Hyelin Han, Assistant Director, Public Policy, Asia Pacific, International Swaps and Derivatives Association, Inc. (ISDA) at hhan@isda.org or +852 2200 5903.

Yours faithfully

A handwritten signature in blue ink, appearing to read "Clifford Chance", is written over the printed name.

Clifford Chance Pte Ltd

Enclosure

TABLE OF CONTENTS

S/N	Description	Page No.
1.	Summary of Major Points	2
2.	Statement of interest	3
3.	Comments	4
	A. Definition of Critical Information Infrastructure	4
	B. Harmonisation of the Bill with Other Legislation and Guidelines	5
	C. Cross-jurisdictional Impact of the Bill	7
	D. Powers of the Commissioner	8
	E. Critical Information Infrastructure	9
	F. Cybersecurity Service Providers	17
	G. Immunity for Disclosure of Information	19
	H. Confidentiality of Information	20
	I. General Comments	21
4.	Conclusion	23

1. Summary of Major Points

We are fully supportive of regulatory reform that will assist in strengthening cybersecurity in Singapore. We also strongly urge the CSA to minimise duplicative, inconsistent and conflicting regulatory requirements and hope that international regulatory coordination continue to achieve cross-border harmonisation.

We understand that many of the proposals in the Cybersecurity Bill are extensive, therefore we hope that sufficient time and consultation will be given for adequate consideration and review of the implementing rules to ensure that there are no unintended consequences and to minimise market disruption and fragmentation.

For example, we request clarification on various definitions set out in the Cybersecurity Bill, such as the definition of "Critical Information Infrastructure" and the interaction of the Cybersecurity Bill with other existing legislations and regulations. Further, we think that the licensing regime for cybersecurity service providers could potentially increase the regulatory burden on corporations and hope that the CSA can provide more information in this regard. Finally, there are certain ancillary issues that we propose be considered in implementing the Cybersecurity Bill such as confidentiality of information, immunity for disclosure of information and liability for disclosing information

We hope that the CSA will consider our comments in the implementation of the Cybersecurity Bill to ensure that compliance costs will not increase significantly for corporations. We welcome further industry discussions and consultation with the CSA and other stakeholders as we move forward in this process.

2. Statement of Interest

ASIFMA, FIA and ISDA (the "**Associations**"), in conjunction with Clifford Chance, welcome the opportunity to provide feedback to the CSA on its Consultation Paper on the Cyber Security Bill and recognise the need for a holistic framework governing cybersecurity.

ASIFMA is an independent, regional trade association with more than 100 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Through the GFMA alliance with SIFMA in the US and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

FIA is the leading global trade organisation for the futures, options and centrally cleared derivatives markets, with offices in London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries as well as technology vendors, lawyers and other professionals serving the industry. FIA's mission is to support open, transparent and competitive markets, protect and enhance the integrity of the financial system, and promote high standards of professional conduct. As the principal members of derivatives clearinghouses worldwide, FIA's clearing firm members play a critical role in the reduction of systemic risk in global financial markets.

Since 1985, ISDA has worked to make the global derivatives markets safe and more efficient. Today, ISDA has over 850 member institutions from 68 countries. These members comprise a broad range of derivatives market participants, including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms, and international and regional banks. In addition to market participants, members also include key components of the derivatives market infrastructure, such as exchanges, intermediaries, clearing houses and repositories, as well as law firms, accounting firms and other service providers.

Given the nature of the businesses of members firms of the Associations, which are largely financial institutions reliant on info-communications technology to manage the financial services they provide, the Associations and their members will inevitably be impacted by the Cybersecurity Bill if any of these services are designated as critical information infrastructure.

The submissions contained therein are limited to derivatives trading, clearing and settlement services.

3. Comments

S/N	Proposal	Comments / Questions
A. Definition of Critical Information Infrastructure		
1.	<p>"Critical information infrastructure" ("CII") is defined to mean a computer or a computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will <i>"lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore"</i>.</p>	<p>We request that the Cyber Security Agency of Singapore ("CSA") consider approaches adopted in other jurisdictions (for example the EU and USA) in providing guidance or a list of factors published which the Commissioner would rely on in deciding whether or not a computer or computer system fulfils the criteria of having a <i>"debilitating impact"</i> on Singapore.</p> <p>The Network and Information Security Directive ("NISD") in the EU provides a list of factors to consider in determining whether an incident (occurring to an operator) would <i>"have significant disruptive effects"</i> on the provision of that particular service. Art 6 of the NISD includes factors such as the number of users relying on the service provided by the entity concerned, dependency of other (critical) sectors on the service provided by that entity and the impact that incidents could have in terms of degree and duration on economic and societal activities or public safety¹.</p> <p>The US Cybersecurity Act 2012 (not passed) provides guidelines for the designation of covered critical infrastructure. The guidelines state that designation may be done if damage or unauthorized access to a system or asset could reasonably result in (i) the interruption of life-sustaining services; (ii) catastrophic economic damage to the USA, including failure of a US financial market; and (iii) severe degradation of national security or national security capabilities. In addition, the Secretary will have to consider the sector-by-sector risk assessments in the designation process.</p> <p>We request that the CSA include such sector-by-sector risk assessments as one of the factors to be considered in designating a CII.</p> <p>We also note that the list of essential services related to financial institutions ("FIs") is</p>

¹ See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC for more information

S/N	Proposal	Comments / Questions
		<p>significantly broader than the equivalent list set out by the EU (see Annex II in the link provided by way of footnote). The EU designates credit institutions (i.e. those engaging in deposit taking activity and operators of trading venues) as essential financial services. The essential services set out by the CSA is broad enough to capture all participants across substantially all of the financial markets of Singapore which effectively reduces the test for CII to one of disruption as noted above. This will create considerable uncertainty going forward. As the designation of CII is subject to the Official Secrets Act, mid-tier firms and banks that do not conduct deposit taking activity in Singapore will have very little guidance to assess whether they may be caught by the regime, and will not have sufficient information available to them to establish any grounds of appealing any such designation.</p> <p>One potential method of determining whether an incident may have significant disruptive effects is to adopt the indicator-based approach adopted by the MAS in respect of the identification of Domestic Systemically Important Banks (or D-SIBs).</p> <p>Further, based on the draft Bill, CII would be specific infrastructure identified and may not be broad enough to cover all the computer systems owned by an FI. We propose that for FIs, a CII identified by the Commissioner should be a subset of critical systems defined under the Technology Risk Management Guidelines and Notice ("TRM") issued by the MAS. Also, we would like to clarify that there is no expectation to undertake a self-assessment to determine which computer systems are CII.</p>
B. Harmonisation of the Bill with Other Legislation and Guidelines		
2.	The Public Consultation Paper mentions that the Bill is a common framework that applies across all sectors but it " <i>recognises that every</i>	We would like to clarify how the Bill would take into account the " <i>unique circumstances of each sector</i> " – whether this would be by way of sector-specific regulations or otherwise. In particular, we would like to clarify if there will be regulations or guidelines specific to services related to banking and finance (as listed in the First Schedule to the Bill), including the payment,

S/N	Proposal	Comments / Questions
	<p><i>CII sector is different</i>", therefore the framework has to be "<i>flexible</i>" in responding to these differences.</p>	<p>derivatives and securities trading, clearing and settlement services industry.</p>
<p>3.</p>	<p>The CSA has informed that it currently works with government lead agencies in charge of each sector ("Sector Leads"), and proposed that the CSA will continue to work with Sector Leads to harmonise regulations in each sector.</p>	<p>We would be grateful if the CSA could clarify if MAS requirements on FIs in relation to cybersecurity would continue to apply to FIs after the Bill is passed, and what would happen if there are conflicting obligations on FIs under the MAS requirements and Bill.</p> <p>We would be grateful if stakeholders in the business of derivatives trading and providing clearing / settlement services could be given an opportunity to be consulted on any changes to MAS regulations and guidelines and on the implementation of the Bill so that the industry has sufficient time adapt to the changes.</p> <p>One possible route forward would be for the CSA to ensure (and expressly provide in the legislation) that a suitable official at each Sector Lead be appointed as an Assistant Commissioner. Each Assistant Commissioner could then also be empowered through delegated authority to issue the relevant rules, regulations and guidelines for each industry. For financial services, the Assistant Commissioner may be an MAS official and the relevant rules, regulations and guidance that would apply may be those of the MAS (although these would in fact be agreed with the CSA in advance). This would reduce the regulatory burden faced by a CHIO, who can continue to refer to a single set of rules, regulations and guidelines.</p> <p>The CSA could continue to harmonise standards and procedures across different industries by working with Sector Leads / Assistant Commissioners and by having appropriate information gathering and investigative powers.</p> <p>We note however that the above approach may not always be suitable. In many instances the CII owners may be unregulated IT infrastructure companies rather than regulated financial services entities, and so relying on the MAS to issue guidelines may not be appropriate in such context. In these circumstances we would suggest the CSA also publish all sector specific guidance under its</p>

S/N	Proposal	Comments / Questions
		own statutory powers.
4.	The CSA has proposed that the Minister may appoint Assistant Commissioners who will, in most cases, come from the Sector Leads, and this prevents CII owners ("CIIOs") from having to report to another regulator.	However, we note that this power is discretionary, and a Minister may not appoint Assistant Commissioners in certain sectors. We would like to clarify if there are other ways to ensure lower compliance costs and more harmonisation within each sector.
C. Cross-jurisdictional Impact of the Bill		
5.	The CSA has proposed that the Bill applies to any CII located wholly or <i>partly</i> in Singapore.	<p>We would like to clarify how would the Bill will affect infrastructure which may be considered as partly in Singapore, but which is in fact part of infrastructure which is located outside Singapore. This is particularly in the context of international or regional firms and organisations – these will have computer systems that are located in Singapore that are connected to computer systems located outside Singapore. What is the test that is to be applied to determine if a computer system is located "partly" in Singapore and how will the Bill interact with potential cybersecurity requirements in other jurisdictions? Similarly, financial market infrastructures such as exchanges, clearing houses and the like will have computer systems that may provide access to firms in Singapore (for example through a terminal). It is unclear whether such connectivity would result in the entire computer system to be subject to the application of the Bill.</p> <p>We strongly believe that there should be no automatic localisation requirements including hardware and data storage if a system is deemed a CII.</p> <p>We are also concerned that the same CII being designated as critical by different regulators across different jurisdictions may create significant conflict of laws risks with respect to outsourcing, confidentiality, bank secrecy and technical standards. We would appreciate if the CSA could</p>

S/N	Proposal	Comments / Questions
		clarify how such conflicts may be resolved.
D. Powers of the Commissioner		
6.	The CSA has proposed that the Commissioner have the power to issue or approve codes of practice or standards of performance which CIOs must comply with.	<p>We would suggest that any such codes of practice or standards of compliance be issued with the following in mind:</p> <p>(a) harmonising such codes of practice and standards of performance with other domestic and international codes and standards may help reduce the compliance burden on organisations;</p> <p>(b) we seek clarification on how the codes of practice and standards of performance will interact with other guidelines, for example, whether such codes or standards will leverage off the MAS TRM. Further, we would like to clarify if the MAS TRM will be consider a code of practice.</p> <p>(c) we suggest that the Commissioner work closely with the MAS to ensure that such codes and standards are consistent with those issued by the MAS and to the extent possible, issue them jointly with MAS. This would be consistent with the clarifications issued as part of the consultation for the Bill.</p> <p>(d) we suggest that for FIs, in the event of a conflict between the codes and standards issued by the Commissioner and the notices and guidelines issued by MAS, that the notices and guidelines issued by MAS should take precedent.</p>
7.	The draft Bill states (at section 21) that the Commissioner has the power to investigate and prevent serious cybersecurity incidents.	<p>We would request the Commissioner to coordinate any investigation and directions to implement remedial measures with other authorities that may be involved in such activities. This is to limit the disruption to organisations.</p> <p>In section 21(2), it is unclear what would constitute a "real" risk. We request further guidance on what constitutes a "real" threat and whether there is a materiality test? There is also a typographical error in section 21(2) – we believe it should read as subsection (1) instead of subsection (2). We ask that consideration be given to systems that support the overseas functions</p>

S/N	Proposal	Comments / Questions
		<p>of an FI and the impact a remedial measure may have on these overseas locations.</p> <p>Given the wide powers of the Commissioner, there should be checks and balances on the exercise of such powers. We propose that for FIs, such powers should be exercised jointly / in consultation with the MAS. Further, there are cross border issues where the information / records contain information of clients who are not contracted to the FI in Singapore, but whose information may be processed in Singapore. We submit that such client information should be excluded from the scope of this section.</p> <p>Also, we would like to clarify how information and records obtained by the Commissioner will be handled and shared during and after its investigations. FIs are bound by banking secrecy and client confidentiality obligations. Any disclosure / leakage of such information to a third party would pose serious reputational and legal risks to us.</p> <p>Further, we would like the Commissioner to clarify what recourse organisations have in the event of a leakage of such information by a government authority.</p>
8.	The draft Bill states (at section 24) that the Minister has certain powers to take emergency cybersecurity measures and requirements.	Given section 24 (application of emergency cybersecurity measures and requirements) read with the definition of CII (section 2), will the application of emergency cybersecurity measures and requirements only apply to CIIs that pass the materiality test for “debilitating impact” on Singapore?
E. Critical Information Infrastructure		
9.	The draft Bill states (at section 7) that a Commissioner " <i>may by a written notice, designate a computer or computer system as a critical information infrastructure for the</i>	<p>The word "<i>may</i>" suggests that the designation of a CII could take place in some other method, besides a "<i>written notice</i>".</p> <p>If the intention is that <i>all</i> CIIOs would receive a written notice notifying them that their computers or computer systems have been designated as a CII, we suggest that the relevant</p>

S/N	Proposal	Comments / Questions
	<p><i>purpose of this Act"</i> (emphasis added in bold).</p> <p>The Public Consultation Paper states (at paragraph 26) that "<i>Section 7 of the Bill will allow the Commissioner to designate a computer or computer system as CII. In doing so, the Commissioner will provide written notice to the owner of the computer or computer system"</i>.</p>	<p>sentence as follows:</p> <p><i>"The Commissioner may, by written notice, designate a computer..."</i></p> <p>The addition of the bold and underlined comma clarifies that the designation is at the discretion of the Commissioner but written notice is required for all designations. We would also like to clarify if a body corporate or corporation may be designated by the Commissioner as a CIIO, after the report of a cybersecurity incident by such body corporate or corporation.</p> <p>Further, we would also like to clarify if a natural person may or would be designated as a CIIO.</p> <p>In addition to the Minister's right to ask for information, a consultation period in advance of any designation would be very valuable to potential CIIOs, as the appeal process that may occur after a CIIO designation is likely to be very formal, and, as mentioned earlier, CIIOs will not have any information on other CIIO designations due to the Official Secrets Act.</p>
10.	<p>The draft Bill defines "<i>owner of a critical information infrastructure</i>" as "<i>a person who (a) has effective control over the operations of the critical information infrastructure and has the ability and right to carry out changes to the critical information infrastructure; or (b) is responsible for ensuring the continuous functioning of the critical information infrastructure</i>".</p>	<p>The proposed definition of "<i>owner of a critical information infrastructure</i>" is broad and it is not clear how it would apply in the context of related corporate entities who may share an information infrastructure. In such instances, would only the parent or holding corporation be designated an "<i>owner of a critical information infrastructure</i>" or would all corporate entities which information are stored in or share the information infrastructure be designated an "<i>owner of a critical information infrastructure</i>" as well? In such an instance, which corporate entity would be designated as the "owner" of the CII? We believe this should not include all corporate entities whose data is stored in the information infrastructure, or which share the use of this information structure as "owners" of the CII. We believe the definition of "owner" requires further clarification as to what may be designated a CII and what this will mean in practice, particularly for cross-border network systems.</p> <p>With respect to a CII which is owned by the Government or a statutory body, the proposed Bill makes clear that the owner shall be deemed to be for example, the Permanent Secretary of the Ministry "<i>having responsibility for the approval of budget and expenditure in relation to the</i></p>

S/N	Proposal	Comments / Questions
		<p><i>critical information infrastructure</i>". We would like to seek clarification on whether a similar approach would be used with reference to privately-owned CIIs. We are concerned and note that a privately-owned company functions differently from a Government entity or a statutory body; the hierarchy in privately-owned companies might not be as clearly defined and CIIs owned by the Government or a statutory body are less likely to be affected by cross-border issues. Therefore, applying a public sector standard to the private sector might not be as appropriate and might increase the scope of compliance for privately-owned CIIs.</p> <p>Does the CSA contemplate that some CIIs may have more than one owner under the definition set out in section 2, for example where one entity has effective control over operations but another entity, which uses the infrastructure on an outsourced basis, has primary responsibility for ensuring the stability of the relevant essential service under applicable laws?</p> <p>If an organisation is not classified as "CIIO" and is compliant with existing laws and local regulations e.g. MAS TRM (e.g. Critical incident report within 1 hour etc.), in-house controls to conduct risk assessments, penetration tests and SOC audits, are there additional requirements to follow?</p> <p>The new law offers the CSA greater power in carrying out remedial measures, such as accessing computers and scanning computers for vulnerabilities. If there is a potential conflict with home site privacy laws, is there any resolution to this conflict and does this greater power extend to non-CII owners?</p> <p>We propose that the contact person be a designation / role rather than a specific person (e.g. the CISO or CIO).</p>
11.	The draft Bill states at section 8 that any person who appears to be operating the computer or computer system may be required to provide information to the Commissioner	<p>We suggest that privileged communications be also exempt from disclosure.</p> <p>Further, we seek clarification on how section 8(2)(c) will operate if there is a conflict of laws. For example, what happens if a CIIO in Singapore processes data for other jurisdictions and is subject</p>

S/N	Proposal	Comments / Questions
	<p>pursuant to a notice, and that any person to whom a notice is issued under section 8(1) is "<i>not obliged to disclose any information where the person is prohibited by any written law from disclosing such information</i>".</p> <p>There are similar provisions at for example, section 11(3) of the draft Bill.</p>	<p>to the confidentiality laws and regulatory requirements of those jurisdictions.</p> <p>We are concerned that the provision setting out the powers of the Commissioner to request information is worded too widely. We therefore suggest that:</p> <p>(a) information requested by the Commissioner should have a nexus to cybersecurity of the computer system;</p> <p>(b) the section include more details and examples of the types of information that the Commissioner may require to be produced;</p> <p>(c) that information requested by the Commissioner should exclude content / data stored in the system (such as customer information); and</p> <p>(d) a check and balance on the exercise of such powers be done through, for example, a requirement that such notices / directions be issued jointly with the MAS. This is in line with the clarifications issued as part of the Consultation.</p>
12.	<p>The draft Bill sets out (at section 10) the duties of a CIIO.</p>	<p>We would like to clarify the transitional period for compliance by a designated CIIO. We note that the Personal Data Protection Act had a transitional period of eighteen months to allow private organisations time to comply, and would suggest a similar timeframe for the Bill.</p> <p>This would provide much needed certainty for designated CIIOs in meeting their compliance requirements such as complying with codes of practice, standards of performance or directions in relation to the CII.</p>
13.	<p>The draft Bill states (at section 10(c)) that a CIIO has the duty to notify the Commissioner of "<i>(i) any cybersecurity incident that occurs in respect of the critical information</i></p>	<p>It would be helpful if there could be further clarification or guidance on the type of cybersecurity incident which needs to be reported to the Commissioner, including the severity and/or impact of incidents which are required to be reported.</p> <p>We believe notification should only be required in the event of significant or material</p>

S/N	Proposal	Comments / Questions
	<p><i>infrastructure; (ii) any cybersecurity incident that occurs in respect of any computer or computer system under the owner's control that is interconnected with or communicates with the critical information infrastructure; and (iii) any cybersecurity incident of a type as prescribed by notification or as specified by the Commissioner".</i></p>	<p>cybersecurity incidents and these terms should be used in a consistent manner.</p> <p>We request that companies should only be required to provide one notification to Singapore authorities in respect of a cybersecurity incident, and that requirements to notify other authorities should be removed under their respective requirements. We propose that for FIs, notifying the MAS of cybersecurity incidents is sufficient and there should not be a need to additionally report to the Commissioner.</p> <p>Regarding section 10(d) and 10(e), we seek clarification on the frequency required to meet “regular” audits or “regular” risk assessments.</p> <p>We wish to clarify if section 10(c) should be read with section 15 and if, under section 10(c), the Commissioner should only be notified of significant cybersecurity incidents (as set out in section 15).</p> <p>We would also like to seek guidance on 10(c)(ii) where the computer system is interconnected with or communicates with CII. As computer systems are increasingly interconnected, the scope of what falls within this definition is unclear. We suggest having examples and assessment criteria to provide guidance.</p> <p>Further, as Singapore may be a hub for security operations in the region, we submit that cybersecurity incidents which occur outside of Singapore, but which are mitigated from or logged in Singapore should not be notifiable.</p>
14.	<p>The draft Bill states (at section 11) that a CIIO has the duty to notify the Commissioner of "<i>material changes to the design, configuration, security or operation</i>" of the CII "<i>not later than 30 days after the changes are made</i>".</p>	<p>Regarding sections 11(a), (b) and (e), if the CII has intellectual property ("IP") such as proprietary source code or operating system that the CIIO does not own, how will the CIIO be protected against any IP infringement as a result of complying with these sections?</p> <p>As noted above, a CIIO in Singapore processes data for other jurisdictions and is subject to the confidentiality laws and regulatory requirements of those jurisdictions. In such an instance, how</p>

S/N	Proposal	Comments / Questions
		<p>will the conflict of laws interact with section 11(4).</p> <p>We would like to suggest that the time period within which such changes must be notified be 60 days instead.</p> <p>We suggest that the phrase "or may potentially affect" in section 11(5) be removed from the definition.</p> <p>We are concerned that this is an onerous obligation and we would like to see more guidance on and examples of what constitutes a "<i>material change</i>".</p> <p>The draft Bill will take precedence over banking and privacy rules that forbid sharing of confidential information - section 11(4) also reflects this. However, section 11(3) allows the owner of CII not to disclose such information where the owner is prohibited by written law. We would like to clarify how these sections are intended to interact with each other. Further, Part 1 of Schedule 3 to the Banking Act contains an exception to banking secrecy if disclosure is necessary for compliance with an order or request made under specified written law. The definition of "specified written law" specifically states the applicable Acts. This definition may need to be amended to take into account the Cybersecurity Act when it is eventually passed.</p>
15.	<p>The draft Bill states (at section 14) that a CIIO must inform the Commissioner of any "<i>intended change in ownership</i>" of the CII "<i>not later than 90 days before the date of the intended change in ownership</i>".</p>	<p>We would like to suggest a different time period for such notification, as 90 days prior to the change in ownership may be impossible in the context of certain merger and acquisitions. We propose not later than 90 days after the <i>actual change in ownership</i> as the change in ownership may involve maintaining secrecy until this is public knowledge.</p> <p>The notification of a change in ownership may be commercially sensitive to organisations (and may attract other obligations where the organisation is publicly traded), and we would request that such information be subject to a heightened level of protection.</p> <p>We would like to see further guidance as to the definition of change in ownership of CII. Is this intended to cover (i) personnel changes, (ii) corporate structure changes, (iii) transfer / sale of CII</p>

S/N	Proposal	Comments / Questions
		<p>to a third party? What is the threshold for notification? We submit that only (iii) should be notifiable to the Commissioner and any internal transfer to an affiliate should be excluded from notification. Further, we propose shortening the notification period to 30 days before the date of intended change, especially since the breach of this section carries criminal liability.</p>
16.	<p>The draft Bill states (at section 15) that a CIIO must establish mechanisms and processes "<i>as may be necessary</i>" in order to detect any cybersecurity threat.</p>	<p>We would like to seek more details and clarification as to the mechanisms and processes "<i>as may be necessary</i>" to detect any cybersecurity threat. Would this include specific computer programs or computer services and if so, how would those be selected?</p> <p>Further, as there may be existing requirements by sector regulators such as the MAS, we seek confirmation that notification requirements under section 15 can be fulfilled by one notification to the sector regulator and there should be no need to additionally report to the Commissioner.</p> <p>Section 15(1), the terms "prescribed period" and "significant" should be defined. We seek clarification on sections 15(1)(a) and (b) as to the meaning of a "significant" cybersecurity incident and how this relates to a "serious" cybersecurity incident which has a severity threshold as defined in section 21(2).</p> <p>We propose that there should be a high threshold for the level of disruption / harm caused by the incident before this reporting obligation is triggered. Also, the threshold should be consistent with other reporting requirements imposed by sector regulators (e.g. MAS reporting including TRM requirements). We also propose that there should be no liability (or at least no criminal liability) for not reporting to the Commissioner if it was internally assessed by the organisation that the cybersecurity incident was not significant.</p> <p>We would also like to seek guidance on section 15(1)(b) where the computer system is interconnected with or communicates with a CII. As computer systems are increasingly interconnected, the scope of what falls within this definition is unclear.</p>
17.	<p>The draft Bill states (at section 7) what is required in the notice designating a</p>	<p>We would like to suggest that the notice issued under section 7 be also required to set out the basis or grounds on which the CII was designated, including how the computer or computer</p>

S/N	Proposal	Comments / Questions
	CII and (at section 18) how any CIIO who is aggrieved by a decision under section 7(1) may appeal and what the appeal should include.	system fulfils the criteria of a CII. This is to assist the decision by any designated CIIO in determining whether an appeal should be lodged and the preparation of any potential appeals.
18.	The draft bill states (at section 16) that CIIOs must conduct cybersecurity audits and risk assessments of CII, and also national cybersecurity exercises will be conducted (section 17).	<p>We request that further guidance on the expected content of a cybersecurity risk assessment be given.</p> <p>As audit and risk assessments are conducted as part of the MAS requirements, we propose that such audit and risk assessments will be deemed to have met the requirements of section 16 of the draft Bill in order to avoid any duplication since FIs regulated by the MAS are required to submit internal audit reports. Section 16(1)(a) states that the Commissioner may appoint or approve an auditor, and we seek confirmation that an FI may use an internal auditor. If an approved external auditor is required, consideration should be given to existing MAS requirements and additional costs an FI will incur. Further, the Commissioner should publish a list of approved external auditors that an FI may use.</p> <p>With regards to section 17(1), we seek clarification on the meaning of a “significant” cybersecurity incident and how this relates to a “serious” cybersecurity incident which has a severity threshold as defined in section 21(2).</p> <p>As the MAS conducts an industry-wide exercise on cybersecurity, will this exercise meet the requirements in section 17? We seek further clarification on what the national cybersecurity exercise will include; for example, will it include a penetration test?</p> <p>We would like to clarify if there is any scope for organisations to use global security firms for such audits or will the Commissioner require the use of security firms which are licensed in Singapore? We submit that that former option allows for consistent standards in the audits that are carried out globally.</p>

S/N	Proposal	Comments / Questions
F. CYBERSECURITY SERVICE PROVIDERS		
19.	The Public Consultation Paper states at paragraph 51 that " <i>in-house provision of cybersecurity services will be exempted from having to obtain a licence</i> ".	<p>We would like to clarify if in-house providers would also be required to comply with certain basic requirements for licensable cybersecurity service providers for example, compliance with a code of ethics or to comply with a "<i>fit and proper</i>" criteria.</p> <p>We suggest that “in-house provision of cybersecurity services” be extended to services provided within a group of companies i.e. affiliates. We understand that cybersecurity service providers would be expected to have compliance regimes in place, however given that in-house cybersecurity service providers operating within a group of companies would already be subject to uniform global group policies, we do not think that these in-house cybersecurity service providers should be treated as cybersecurity service providers which have to be licensed.</p> <p>We suggest that the Bill provide an exclusion for cybersecurity service providers which continue to provide such services on a transitional basis to entities which were formerly affiliated but have since been sold or otherwise spun off from a corporate group. We note that an obligation to ensure a smooth transition is often required under regulatory rules and obtaining a licence for such a temporary activity may be counter-productive.</p>
20.	The Public Consultation Paper states at paragraph 56 that " <i>the same licensing requirements will apply to such overseas providers</i> ".	<p>We suggest that the draft Bill expressly states that such licensing requirements would apply to overseas providers as well.</p> <p>We believe that any licensing requirements for an overseas provider should not automatically result in localisation requirements including hardware and data storage or be too onerous such that overseas providers do not want to provide their services to Singapore market participants as the licensing requirements outweigh the benefits of providing services to Singapore market participants. Further, we are of the view that services provided by an FI's affiliates should not be required to attain a license as the FI would already be subject to oversight by the MAS.</p>
21.	The Public Consultation Paper states	We are concerned that the designation of a computer or computer system as a CII being an

S/N	Proposal	Comments / Questions
	<p>at paragraph 28 that <i>"[t]he designation of a computer or computer system as a CII is an official secret under the Official Secrets Act, and shall not be divulged to the public"</i>.</p>	<p>official secret would subject organisations to onerous obligations under the Official Secrets Act which may be difficult especially for large organisations to comply with. We suggest that organisations be afforded sufficient and relevant exemptions (including those which are industry-specific) to ensure that compliance with such requirements is not unduly onerous.</p>
22.	<p>The draft Bill requires service providers to be licensed (sections 26 and 29).</p>	<p>The definition of non-investigative cybersecurity service in section 25 is very broad and may potentially cover all services, particularly limb (d), which states “assessing or monitoring the compliance of an organisation with the organisation’s cybersecurity policy”. Section 25(d) may potentially capture all services provided as an organisation’s cybersecurity may apply to all parts of the organisation.</p> <p>For investigative cybersecurity providers which are located overseas or are global service providers, we believe there should be a balance between the need to protect the Singapore market and discouraging / preventing Singapore market participants from engaging an overseas service provider or a global service provider. Care should be taken that the licensing regime for both non-investigative cybersecurity and investigative cybersecurity will not result in the unintended consequence of requiring an overseas service provider or a global service provider to have a significant local presence. This would be detrimental to both the level of service a Singapore market participant may have access to as well as the increased costs a Singapore market participant may face.</p> <p>In the event that there are existing certification requirements by the MAS, how will these certification requirements interact with the licensing requirements in the Bill? We suggest using industry certifications as the basis for licensing and to reduce the time taken to attain a license.</p> <p>We seek confirmation that in-house staff will not be required to have a license as per section 26(3). A license will only be required if the organisation employs an individual that supplies cybersecurity services, i.e., a pen tester employed for an in-house team will not be required to get a license. For contract staff that are hired using a managed service model, will this person(s) be</p>

S/N	Proposal	Comments / Questions
		<p>required to have a licence?</p> <p>Institutions need flexibility when they select qualified vendors to perform security services e.g. pen test, SOC monitoring, especially for MNCs which may appoint reputable vendors not in the CSA's list of licensed service providers. We suggest allowing FIs to use their discretion as long as the vendors have professional qualifications and experience in order to avoid the onerous licensing requirement.</p> <p>We would like to see further guidance / directions from the Commissioner on when licensed service providers must be engaged. We propose that the use of global cybersecurity service providers which are not licensed in Singapore should be allowed if the solutions / services are not targeted at Singapore specifically (e.g. for global monitoring or penetration testing services). Further, this allows for consistent standards in the services (e.g. audits) that are carried out globally.</p>
G. IMMUNITY FOR DISCLOSURE OF INFORMATION		
23.	<p>The draft Bill (at sections 20(5), 24(3) and (7)) provide immunity to obligations of non-disclosure under law in the event where (i) a person is examined by a cybersecurity officer or (ii) complying with emergency measures.</p>	<p>The Bill does not provide immunity to obligations of disclosure for information disclosed to the CSA on a voluntary basis. Given that information sharing is likely to be beneficial to both the CSA and the party sharing the information, a general immunity clause for information shared in good faith would be beneficial. A potential possibility with extending immunity to the CSA is that it can then become a "clearing house" of cyber threat and cyber-incident information sharing.</p> <p>We suggest drafting a general provision to provide immunity from law for disclosure of information, in good faith, for the purposes of sharing information relating to a cybersecurity threat or a cybersecurity threat / incident. Such immunity should cover the particular act of disclosure and not any other non-compliance with law to prevent abuse.</p>

S/N	Proposal	Comments / Questions
H. CONFIDENTIALITY OF INFORMATION		
24.	The draft Bill (at section 48) requires a person to preserve secrecy of certain matters specified	<p>It is unclear whether the scope of section 48 of the Bill would be sufficient to preserve confidentiality of commercially sensitive information such as pre-patent ideas or trade secrets. In particular:</p> <ol style="list-style-type: none"> 1) Section 48(8) only imposes confidentiality obligations on authorised persons and not relevant organisations. 2) It is unclear what mechanism (if any) exists for the Commissioner to consider the grounds by which he may accept / reject the rationale set out in the written statement required by Section 48(5). 3) Section 48(6) does not provide for a mechanism by which the Commissioner's decision to disclose information can be judicially challenged beyond administrative / judicial review, nor whether there is an avenue for the courts to grant protective orders for information that is sought to be disclosed. 4) It is unclear if Section 48 covers voluntary disclosure. <p>Following on from the above, we suggest that the draft Bill be amended to grant clearer confidentiality processes such as:- (1) pre-notification where the Commissioner wishes to disclose commercially confidential information; (2) grounds on which the Commissioner assesses the written statement or which the decision to disclose can be challenged; (3) a general obligation of confidentiality from the CSA and the disclosed information that goes beyond "specified persons"; and (4) an obligation of confidentiality to be imposed under Section 48 when there is voluntary disclosure.</p> <p>Will there be guidelines or platforms developed for the sharing of cybersecurity information and what is the data protection mechanism? Will the MCI/CSA consider instituting intelligence</p>

S/N	Proposal	Comments / Questions
		platforms specific to certain sectors?
I. GENERAL COMMENTS		
25.	Part 6 (General) Section of the draft Bill	<p>Officers/employees performing their day to day duties in good faith, except where there is wilful neglect, should not incur criminal liability even if the corporate entity commits an offence. We suggest using similar wording to section 48 of the Personal Data Protection Act 2012 as reproduced below:</p> <p>48. Defence for employee</p> <p>(1) In any proceedings for an offence under this Part brought against any employee in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by the employee, it is a defence for the employee to prove that he did the act or engaged in the conduct in good faith</p> <p>(a) in the course of his employment; or</p> <p>(b) in accordance with instructions given to him by or on behalf of his employer in the course of his employment.</p> <p>(2) Subsection (1) does not apply to an employee who, at the time the act was done or the conduct was engaged in, was an officer and it is proved —</p> <p>(a) the act was done or the conduct was engaged in with the consent or connivance of that officer; or</p> <p>(b) the act done or the conduct engaged in was attributable to any neglect on the part of that officer.</p>

S/N	Proposal	Comments / Questions
		(3) In subsection (2), “officer” has the same meaning as in section 52(5).

4. Conclusion

We thank you for this opportunity to respond to the Consultation Paper and the proposed Cybersecurity Bill and we are, of course very happy to discuss with you in greater detail any of our comments. We hope that the comments will be considered in implementing the Cybersecurity Bill.