31 May 2022

To:
China Securities Regulatory Commission (CSRC)
Submitted by email to kejiju@csrc.gov.cn and by fax to 010 880614444

ASIFMA response to CSRC consultation on Cybersecurity Measures in Securities and Futures Industries

Dear Sir/Madam,

The Asia Securities and Financial Markets Association ("ASIFMA")[1] appreciates the opportunity to respond to China Securities Regulatory Commission's (the "CSRC") consultation paper on Cybersecurity Measures in Securities and Futures Industries (Measures). ASIFMA's submission consists of two sections: 1) General comments; and 2) Specific comments on an article-by-article basis.

General Comments:

Alignment with existing rules and regulations
We recommend that the Measures align with existing regulatory requirements to avoid confusion by regulated entities. As pointed out in the detailed article-by-article comments further below, many requirements in the draft Measures focus on stress testing, performance requirements and enhanced data backup requirements for certain data types in the CSRC Information Technology Management Measures which took effect in 2019 (amended in 2021) but divert from existing regulatory requirements.

Risks of sharing sensitive data
The draft Measures focus on data security; however, but also require the sharing of data for various purposes in Article 29, 50 and 52. Enhancing data security is important for all parties, particularly those who are given access to or custody of sensitive data and information. Certain data, particularly cybersecurity-related info, is highly sensitive to operating institutions, and the data is extremely useful to hackers and other bad actors and could enable such actors to target the operating

[1] ASIFMA is an independent, regional trade association with over 160 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. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.

institutions and/or the industry directly or through supply chain. Therefore, we would like to work with the CSRC to minimize data collection, reduce electronic footprint and seek alternative ways if sensitive data is absolutely needed to be collected for supervisory purposes. We refer to our letter on this topic that was sent to Mr Shen Bin (Director General, Department of International Affairs, CSRC) on 14 September 2021, in his capacity as vice-chair of the IOSCO Asia Pacific regional committee (see Annex A).

Pen-testing requirement

Article 52 states CSRC and its commissioned third party could conduct pen-testing and system scanning on core institutions and operating institutions. The same requirement is also included in CSRC's Information Technology Management Measures (Article 56).

We understand CSRC's interest in obtaining a better assessment of core institutions and operating institutions' cyber security programs and strengths and weakness in their defenses through independent testing. However, regulator-led or regulator-commissioned third-party-led penetration testing could be unsafe to firms and the sector as the tests pose real risks to firms due to the potentially disruptive nature of penetration testing and the sensitivity of testing results. Testing systems and applications without operational context could create significant disruption to firm operations. Testing provides a point-in-time assessment of a specific vulnerability. It is only one of many tools a firm uses as part of a mature "defense-in-depth" approach to evaluating risk and the efficacy of controls and will not provide the comprehensive view in terms of assurance of a firm's overall security posture.

We recommend that the CSRC reconsider the approach in Article 52 and in Article 56 of the existing CSRC's Information Technology Management Measures, recognize firm-led pen-testing and scanning, allow firms opportunity to share its approach to vulnerability management, and work with operating institutions to identify alternative approaches that operating institutions could demonstrate their cybersecurity capability.

Regulating IT Service Providers

We note the draft Measures included a proposal to directly regulate the activities of IT service providers alongside regulated firms and this is also the approach taken in the CSRC's Information Technology Management Measures. Globally, information technology service providers are not licensed or regulated by financial services industry regulators, and financial regulators require regulated entities to seek, via contractual or other means, adequate controls, reporting obligations, and access to information from the IT service providers that they use. We suggest that the CSRC aligns with global regulatory practice and adopts such an approach rather than seeking this information from the IT service providers directly. As such, CSRC will preserve the spirit of the regulation and fulfill what we understand to be the objectives underpinning the regulation, whilst keeping the compliance obligations on the firms that CSRC regulates.

Sector-wide Strategic Data Backup

We note the requirements for sector-wide data backup. We submit that core institutions and operating institutions should be responsible for their own data backup following global standards and industry best practice sand should not rely on an industry-wide strategic data backup center for cyber incident response and recovery (CIRR).

Furthermore, as highlighted above, there are significant risks associated with sharing of data, particularly data sensitive to firm's cybersecurity as the data is extremely useful to hackers and other bad actors and could enable such actors to target the operating institutions and/or the industry directly or through supply chain.

Lastly, sector wide strategic data backup center present a concentration risk to the industry and could be a one-stop database of valuable data for hackers and malicious actors. This not only poses huge risks to all core institutions and operating institutions on an individual basis, but also brings significant systemic risks for the sector in China and globally given the inter-connectedness of the global financial sector, if the data is compromised or leaked.

Therefore, we recommend CSRC to encourage firms to enhance its own CIRR capability by using international standards and best practice such as the Financial Sector Profile (or Cyber Risk Institute Profile or FSP)[2], and refrain from creating a single point of failure for the whole sector if compromised.

A risk-based and principles-based approach

We urge CSRC to focus on encouraging FIs to make use of a risk-and principles-based cybersecurity framework that could be appropriately applied to all financial market participants regardless of size. The global financial industry created the Financial Sector Profile (or Cyber Risk Institute Profile or FSP), a cyber risk management assessment tool that the industry created which allows an organization to diagnose cyber risk and apply relevant standards and best practices to appropriately manage that risk. FSP adopts a tiering mechanism that serves as a scaling device to customize the Profile based on an individual institution's risk and activities. Four categories of impact are most reflective of the institution's impact: National, Subnational, Sectoral, or Localized. As an example, tier 1 institutions with national impacts are expected to assess against 277 diagnostic statements while tier 4 institutions with localized impact need only to answer to 137 diagnostic statements. FSP synthesizes the best cyber practices from industry, as well as regulators in different jurisdictions. We believe adoption of the FSP by FIs and recognition of the FSP by CSRC would increase global regulatory harmonization and elevate the sector's cyber posture as well as make communication between firms and competent authorities in China more effective. CSRC could benefit from the standardized risk assessment tool to better discern the sector's systemic risk with more time for jurisdictional specialization.

In addition to the above general comments, we submit specific feedback on some of the Articles in the draft Measures in the following pages.

We sincerely hope the CSRC will positively consider our recommendations. We remain at your disposal should you have any questions and would welcome the opportunity to discuss during a virtual meeting.

Sincerely,

Laurence Van der Loo

Executive Director, Technology & Operations

Asia Securities Industry & Financial Markets Association

General Comments: see next page

Specific Article	Article details	ASIFMA Comments
Article 7	China Securities Association, China Futures Association, and China Securities Investment Fund Association (hereinafter collectively referred to as industry associations) shall formulate industry cybersecurity self-discipline rules in accordance with the law. Implement self-discipline management of cybersecurity for operating institutions.	• We recommend that the self-discipline rules are developed following the principles of transparency, openness, impartiality and consensus, effectiveness and relevance, coherence. We would like to confirm with CSRC that operating institutions could voluntarily participate to industry associations' self-discipline management program. We suggest to revise the article 7 to the following: "China Securities Association, China Futures Association, and China Securities Investment Fund Association (hereinafter collectively referred to as industry associations) can formulate industry cybersecurity self-discipline rules in accordance with the law following the principles of transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and operation institutions could join the industry self-discipline program voluntarily. Industry associations could implement self-discipline management of cybersecurity for participating operating institutions."
Article 13	Core institutions and operating institutions shall ensure that information systems and related infrastructure have a reasonable structure, sufficient performance, capacity, reliability, scalability, and security, and ensure that relevant security technical measures are planned and planned synchronously with informatization work. Simultaneous construction and simultaneous use. The performance capacity of the information system	• The key term "performance capacity" is not clearly defined. Does it mean overall system capacity or single capacity indicator (like) CPU, disk, etc.)? The value for "historical peak" could be dynamic. We request the CSRC to clarify whether that means that the performance capacity needs to be adjusted very frequently to ensure it is always not less than twice the historical peak. If this is the case, it is challenging for firms to constantly adjust or expand capacity needs. • We recommend that the draft Measures align with the requirements in CSRC's Information Technology Management Measure, focus on important information systems and adopt a risk-based and principle-based approach and not prescribe technology performance.

	shall not be less than twice the historical peak.	Article 23 of CSRC's Information Technology Management Measures states: "Securities and fund companies shall regularly conduct stress tests, assessments and analyses on important information systems in combination with the companies' development strategies, market trading size and other factors in order to ensure that their capacity can meet the business demand." We recommend to revise the article 13 of the draft Measures to the following to align with CSRC Information Technology Management Measures: "Article 13: Core institutions and operating institutions shall ensure that information systems and related infrastructure have a reasonable structure, sufficient performance, capacity, reliability, scalability, and security, and ensure that relevant security technical measures are planned synchronously with informatization work and simultaneous constructed and used. Core institutions and operating institutions shall ensure that the capacity of the important information system can meet the business demand. ~~The performance capacity of the information system shall not be less than twice the historical peak."~~
Article 15	Core institutions and operating institutions shall conduct risk assessments and conduct adequate tests if they newly build, operate, or remove important information systems, and formulate emergency response and rollback plans; those that may have a greater impact on the safe and stable operation of the securities and futures market shall be reported to the China Securities Regulatory Commission and its	• We recommend consistency with existing requirements and hope that the draft measures align with the change management notification requirements in CSRC's Information Technology Management Measures and in the event of newly building or replacing the computer room where an important information system is located or the information system relating to securities and fund trading, securities and fund companies shall submit relevant materials to CSRC within 5 working days prior to relevant business activities, including opinions of internal reviews, basic information of computer room, technical structure design, operational processes, information security

	dispatched offices in advance.	management materials, business system, compliance management, risk management system, etc.
Article 17	Core institutions and operating institutions shall establish and improve cybersecurity monitoring and early warning mechanisms, set monitoring indicators, continuously monitor the operation of information systems and related infrastructure, deal with abnormal situations in a timely manner, and conduct regular assessments of the monitoring mechanism's implementation effect and continue optimization. Core institutions and operating institutions shall comprehensively and accurately record and properly preserve business logs and system logs in the process of production and operation to ensure that they meet the needs of failure analysis, internal control, investigation, and evidence collection, etc. The retention period of business logs shall not be less than twenty years, and the retention period of system logs shall not be less than six months.	• The 20-year record-keeping requirement could be challenging, and we hope the CSRC can share the rationale behind this requirement. • The Securities Law (2019)[3] laid out comprehensive retention requirements for customers' materials for opening accounts, entrustment records, transaction records and all the information relating to internal management and business operations. We recommend the draft measures to be aligned with the scope in the Securities Law and remove the undefined "business logs".
Article 18	Core institutions and operating institutions shall establish intra-city and	• CSRC's Information Technology Management Measures comprehensively laid out requirements on data backup and have set

3

	remote data backup facilities, back up data at least once a day, and verify the validity of data backup at least once a quarter. Core institutions and operating institutions shall establish failure backup facilities and disaster backup facilities for information systems and determine recovery goals according to the importance and scope of influence of the information system to ensure business activities continue. Disaster backup facilities shall be embodied in the form of disaster backup centers in the same city or in different places. Where core institutions and operating institutions adopt an active-active or multi-active architecture to deploy important information systems, and on the premise that the business continuity operation capability is not lower than the provisions of the preceding paragraph, any data center may be regarded as a disaster backup facility for other data centers.	out CSRC's expectation on this front. We would like to confirm the requirements in the draft measures are consistent with data backup requirements in the IT Measures and recommend the draft Measures to consistently align with IT Measures in wording and approaches to reduce confusions and misunderstanding.
Article 19	Core institutions and operating institutions shall conduct stress testing of important information systems at least every six months, formulate stress testing plans and set test scenarios based on the	• We suggest that global FI's can leverage and rely on existing testings done Globally or Regionally. • This article requires stressing testing of important systems. We would like the CSRC to clarify the stress testing requirements and whether the definition of "important

	technical characteristics of the system and the type of services it carries. Set up test indicators for equipment construction and other aspects, organize the test work in an orderly manner, and form a stress test report for archiving after the test is completed. Core institutions and operating institutions shall, in accordance with relevant requirements, participate in the industry-wide stress test of important information systems organized by the China Securities Regulatory Commission, and rectify in a timely manner based on the test results; if rectification is temporarily impossible, a feasible rectification plan shall be formulated.	information system" is consistent with the CSRC IT Management Measures. • We recommend that the draft Measures align with the requirements in CSRC's Information Technology Management Measures and adopt a risk- and principle-based approach and not prescribe technology performance. Article 23 of CSRC's Information Management Measures states: "Securities and fund companies shall regularly conduct stress tests, assessments and analyses on important information systems in combination with the companies' development strategies, market trading size and other factors in order to ensure that their capacity can meet the business demand." We suggest revising the article 19 to the following to align with CSRC Information Technology Management Measures: "Article 19 Core institutions and operating institutions shall conduct stress testing of important information systems regularly ~~at least every six months~~, formulate stress testing plans and set test scenarios based on the technical characteristics of the system and the type of services it carries. Set up test indicators for equipment construction and other aspects, organize the test work in an orderly manner, and form a stress test report for archiving after the test is completed."
Article 20	Information technology service institutions shall file with the CSRC in accordance with the law and provide information technology products or services for securities and futures business activities in accordance with relevant business rules. Core institutions and operating institutions shall establish and improve internal management	• As highlighted in the general comments, we recommend CSRC to align with general global practice that requires regulated entities to seek, via contractual or other means, adequate controls, reporting obligations, and access to information from the IT service providers that they use.

	mechanisms, improve access standards for information technology products and services, prudently purchase and continuously evaluate the quality of relevant products and services, strengthen confidentiality management, improve risk management measures in a timely manner, and improve emergency response mechanisms to ensure Safe and smooth operation of the institution's network security and related businesses.	
Article 21	Core institutions and operating institutions shall strengthen the construction of independent research and development capabilities, continuously improve their independent and controllable capabilities, and carry out information technology application innovation work in accordance with the relevant requirements of the state and the China Securities Regulatory Commission.	• We request the CSRC to clarify whether "independent and controllable capabilities", is referring to usage of internal development vs. outsourcing, or from cross broader perspective? • We recommend that the draft Measures adopt a technology neutral approach and allow companies the flexibility to choose technology that best suits their business and operational needs.
Article 23	(5) Build a data quality assessment framework and establish a quality control and accountability mechanism.	• Item 5 mentions establishment of data quality assessment framework, quality control and accountability mechanism. We seek clarification from the CSRC on data quality framework, such as best practices of such framework and mechanisms.
Article 24	When core institutions and operating institutions handle important data and core data, they shall	• Article 24 requires that systems processing of important data should satisfy L3 above requirement of Multi-level Protection

	specify the person in charge of data security in accordance with the law and designate a data security management institution or department. In principle, the information systems of core institutions and operating institutions that process important data shall meet the requirements for the protection of network security levels above level 3, and the information systems that process core data shall be strictly protected in accordance with relevant laws and regulations.	Scheme (MLPS). Does it mean system could be classified as L2, but satisfies L3 requirements? • MLPS Regulations (2018 draft) establish the criteria and process for MLPS classification and should be followed as the authoritative guidance when it comes to MLPS classification. We recommend the CSRC measures reference the draft MLPS Regulations for classification criteria and remove the additional criteria on "important data" to keep the rules consistent. We suggest revising article 24 to the following: "Article 24: When core institutions and operating institutions handle important data and core data, they shall specify the person in charge of data security in accordance with the law, and designate a data security management institution or department. The information systems that process core data shall be strictly protected in accordance with relevant laws and regulations."
Article 26	Core institutions and operating institutions may process PII without obtaining individual's consent where it is necessary to perform a statutory responsibility, statutory obligation, or regulatory requirements.	• We suggest to keep the wording consistent with the Personal Information Protection Law (PIPL). The term "regulatory requirements" is very generic and might therefore broaden the scenarios under PIPL which may cause some uncertainty in practice. • As such, we suggest CN: 为履行法定职责、法定义务~~或者监管要求所必需~~，核心机构和经营机构可以在未取得个人同意的情况下，处理个人信息。 • EN: Core institutions and operating institutions may process PII without obtaining individual's consent where it is necessary to perform a statutory responsibility, statutory obligation, ~~or regulatory requirements~~.
Article 28	No institution or individual may conduct activities such as certification, testing, risk assessment, etc. of important	

	information systems in the securities and futures industry in violation of regulations and may not release cybersecurity information such as system vulnerabilities, computer viruses, network attacks, and network intrusions to the public in violation of regulations.	
Article 29	The CSRC may designate relevant institutions to build a strategic backup data center for the securities and futures industry, carry out centralized backup and management of industry data, and continuously improve the securities and futures industry's ability to respond to major disasters. Core institutions and operating institutions shall submit data to the Securities and Futures Industry Strategic Data Backup Center in a timely manner in accordance with regulations, and the submitted data must be true, accurate and complete.	• We suggest that global FIs should be allowed to leverage existing backup data Centers Globally or Regionally. • As highlighted in the general comments, we would like to submit that Core Institutions and Operating Institutions should be responsible for their own data backup following global standards and industry best practice and should not rely on an industry wide strategic data backup center for CIRR. Furthermore, as highlighted in the general comments, there are significant risks associated with sharing of data, particularly data sensitive to firm's cybersecurity as the data is extremely useful to hackers and other bad actors and could enable such actors to target the operating institutions and/or the industry directly or through supply chain. Therefore, we would like to work with the CSRC to minimize data collection, reduce electronic footprint and seek alternative ways if sensitive data is absolutely needed for supervisory purposes. Lastly, sector wide strategic data backup center presents a concentration risk to the industry and could be a one-stop data base of valuable data for hackers and malicious actors. This not only poses huge risks to all core institutions and operating institutions on an individual basis, but also brings significant systemic risks for the sector in China and globally given the inter-connectedness of the global financial sector, if the data is compromised or leaked.

		Therefore, we recommend CSRC to encourage firms to enhance its own CIRR capability by using international standards and best practice such as Cyber Risk Institute's Profile and refrain from creating a single point of failure for the whole sector if compromised.
Chapter 4	**Cybersecurity Emergency Response**	• We suggest the draft measures to align requirements with 2021 CSRC Measures on Cybersecurity Incident Reporting, Investigation and Handling in the Securities and Futures Industry on cybersecurity incident response related requirements.
Article 30	Core institutions and operating institutions shall establish a cybersecurity risk monitoring and early warning mechanism, strengthen daily monitoring, and regularly conduct vulnerability scanning, security assessment, and other work. If core institutions, operating institutions and information technology service institutions find that network security products or services have security defects, system loopholes and other hidden dangers, they shall promptly verify and rectify them; The CSRC and its dispatched agencies report. The China Securities Regulatory Commission and its dispatched offices may conduct industry reports on relevant security defects, system vulnerabilities and other hidden dangers, and core institutions, operating institutions and	• We suggest that global FIs should be allowed to leverage and rely on existing risk monitoring and vulnerability scanning routines performed Globally or Regionally.

	information technology service institutions shall investigate and take risk prevention measures in a timely manner.	
Article 41	The CII entities in the securities and futures industry shall continuously monitor the safe operation of critical information infrastructure, conduct regular stress tests, and if system performance and network capacity are found to be insufficient, they shall promptly take measures such as system upgrade and capacity expansion to ensure that The system performance capacity shall not be lower than three times the historical peak value, and the network bandwidth shall not be lower than twice the historical peak value.	• The value for "historical peak" could be dynamic. We request the CSRC to clarify whether this means the performance capacity needs to be adjusted very frequently to ensure it is always not less than three times the historical peak for CII entities? If this is the case, it is challenging for firms to constantly adjust or expand capacity needs.
Article 46	Core institutions may apply for national professional qualifications to carry out cybersecurity certification, testing, testing, and risk assessment in the securities and futures industry. Relevant core institutions shall ensure sufficient resource input, improve internal management, and work processes, and ensure work professionalism, independence, and credibility. The China	• We appreciate CSRC's support to Core Institutions and their affiliates in applying national professional cybersecurity qualifications to carry out cybersecurity testing, certification, and assessment for cybersecurity supervision work in securities and futures industry. We would like to seek confirmation that firms could also leverage national entities with right cybersecurity qualifications for cybersecurity certification, evaluation, and testing.

	Securities Regulatory Commission regularly evaluates the work carried out by the core institutions in the preceding paragraph. If the evaluation passes, it may be used as a support unit for cyber security supervision in the securities and futures industry. The relevant work progress can be used as a reference for the implementation of supervision and management by the China Securities Regulatory Commission and its dispatched offices.	
Article 49	Industry associations shall encourage and guide the innovation and application of cybersecurity technologies, enhance their independent and controllable capabilities, organize, and carry out scientific and technological awards, and promote the scientific and technological progress of the industry. Industry associations should guide information technology service agencies to participate in industry cybersecurity and informatization work in a standardized manner and promote fair competition in the market.	• We recommend that the draft Measures adopt a technology-neutral approach and allow companies the flexibility to choose technology that best suits their business and operational needs.
Article 50	The CSRC and its dispatched offices may require core institutions, operating institutions, and information technology service institutions to	• As highlighted in the general comments, we would like to work with the CSRC to ensure that the cybersecurity-related data requested are not sensitive in nature and data is handled in a safe and secure manner. If

	provide information and data related to cybersecurity management in the securities and futures industry. Relevant institutions shall cooperate and provide relevant materials in a timely, accurate and complete manner.	sensitive data is absolutely needed for supervisory purpose, we encourage CSRC to minimize electronic data collection and explore alternative methods such as onsite sighting of the data by regulators at the firm's premises to reduce the risk. We would suggest to revise the article to the following: "In order to fulfil its duties under these Measures, the CSRC and its dispatches offices may require Core Institutions, Operating Institutions, and information technology service institutions to provide timely materials related to cyber security management of the securities and futures industry, and the materials provided shall be true, accurate, and complete, in accordance with the provisions of law and administrative regulation".
Article 52	The CSRC and its dispatched offices may authorize national or industrial professional institutions to assist in the supervision and inspection of core institutions, operating institutions and information technology service institutions via penetration testing, vulnerability scanning and other information technology risk assessment.	• We strongly recommend the article be removed. • We understand CSRC's interest in obtaining a better assessment of core institutions and operating institutions' cyber security programs and strengths and weakness in their defenses through independent testing. However, conducting penetration testing could be unsafe to firms and the sector as the tests pose real risks to firms due to the potentially disruptive nature of penetration testing and the sensitivity of testing results. Testing systems and applications without operational context could create significant disruption to firm operations. Testing provides a point-in-time assessment of a specific vulnerability. Regardless of how extensive or sophisticated a test might be, it is only one of many tools a firm uses as part of a mature "defense-in-depth" approach to evaluating risk and the efficacy of controls. It will not provide the comprehensive view in terms of assurance of a firm's overall security posture. We recommend that the CSRC recognize firm-led pen-testing and scanning, and work with operating institutions to

		identify alternative approaches that could demonstrate their cybersecurity capability. • We also suggest that FIs should be allowed leverage and rely on existing inhouse Pen testing conducted Globally or Regionally.
Article 62	(5) Important data and core data refer to the important data and core data determined in accordance with the Data Security Law and the relevant data classification and grading protection system of the state and the securities and futures industry.	• Item 5 mentions important data and core data refer to the data as defined in the Data Security Law and the relevant data classification and grading protection system of the state and the securities and futures industry. Currently, the definition and scope of key terms and data classification work remain unclear. We recommend CSRC work in consultation with industry when drafting guidance on data classification or defining the scope of key terms such as “important data” or “core data” and ensure an open, transparent and inclusive drafting process.