The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 34143

May 17, 2022

China Proposes Draft Cybersecurity Rules for Securities and Futures Industry

[34143]

May 17, 2022

TO: ICI Global Members
Global Regulated Funds Committee
Global Regulated Funds Committee - Asia SUBJECTS: International/Global
Operations RE: China Proposes Draft Cybersecurity Rules for Securities and Futures Industry

On 29 April 2022, the China Securities Regulatory Commission (CSRC) released for public consultation the Measures for the Administration of Cybersecurity Relating to the Securities and Futures Industry (Draft for Comments) ("Draft Measures").[1] It is open for public comment until 29 May 2022. ICI Global will track this consultation but does not intend to comment.

The Draft Measures aim to provide the operational details for the securities and futures industry on implementing the general legal requirements under China's three-pronged regulatory framework on information security, namely, the Cybersecurity Law,[2] the Data Security Law (DSL)[3] and the Personal Information Protection Law (PIPL).[4]

The Draft Measures will apply to three types of institutions:

- operators of financial market infrastructure (e.g., securities and futures exchanges);[5]
- securities and futures business institutions, which include fund management companies, among others;[6] and
- information technology companies that provide services for securities and futures business activities.

Global asset managers who set up fund management companies (FMCs) in China will be expected to observe the proposed requirements on network security and data protection. This memorandum briefly summarizes the major proposed requirements in the Draft Measures that will be applicable to FMCs.

Network Security Governance

General Requirements

By way of background, the Cybersecurity Law requires institutions to establish network security policy and operation procedures, designate network security personnel, and monitor and trace network activities and incidents. The Draft Measures set out further details on these general requirements.

The Draft Measures stipulate that the person in charge of an FMC should take primary responsibility for network security, and the person in charge of information technology should be assigned as the Directly Responsible Individual for network security. Further, an FMC should designate a dedicated division or department to manage and monitor its important information systems, as well as prepare a contingency plan and carry out emergency drills and exercises, at least annually, to deal with network security incidents.

In line with the Cybersecurity Law, FMCs should adopt the Multi-Level Protection Scheme (MLPS)[7] in assessing the technology systems and risks. FMCs should file with the CSRC once they define the protection level for their network security and notify the CSRC on any changes of the defined protection level.

The Draft Measures will also require FMCs to establish intra-city and remote data backup facilities. FMCs should backup their data at least once every day and validate the backup data at least once every quarter. To ensure business continuity in the event of server failure or disasters, FMCs should set up information system backup facilities, as well.

Additional Requirements for Critical Information Infrastructures (CIIs)[8]

FMCs that operate CIIs will be subject to additional requirements on network security. They should assign a division or department, with at least five network security personnel, dedicated to the security management of CIIs. Such division or department should carry out security background screening on its network security personnel. Also, there should be a dedicated network security officer assigned to each CII. These FMCs should conduct at least one network security test and risk assessment of their CIIs every year.

Data Security Protection

The Draft Measures outline a list of measures that FMCs should implement to comply with the data security requirements under the DSL. An FMC should establish a comprehensive data security management system and formulate a data access control policy, which allocates access rights based on the principle of least privilege. In addition, using relevant industry standards, it should set up a mechanism to classify its business data in order to adopt the MLPS when discharging the data security protection obligations, as required under the DSL.

For FMCs processing "important data" and "core data",[9] they should appoint a data security officer and designate a management department to take the responsibilities for data protection. Any system that processes "important data" must hold above level 3 MLPS certification, whereas a system processing "core data" must enforce stringent security measures pursuant to applicable regulations.

Processing of Personal Information[10] of Investors

On the processing of personal information, the Draft Measures reiterate that FMCs should

obtain consent from their investors, and clearly inform the investors of the purpose and methods of the data processing. Moreover, FMCs should obtain separate consent from the investors in case of (i) processing sensitive personal information, including securities and futures accounts, or (ii) sharing or disclosure of personal information.

Annual Reporting

By 30 April each year, the FMCs should complete an evaluation of their network security work in the previous year and submit a network security management report to the CSRC. The report should cover the network security governance, dedicated personnel, risks, and next year's work plan. FMCs who operate CIIs should also include in the report the result of the network security test and risk assessment of their CIIs.

Lisa Cheng
Research Analyst
ICI Global

endnotes

[1] Administrative Measures for Cybersecurity Relating to the Securities and Futures Industry (Draft for Comments), 29 April 2022, available (in Chinese only) at http://www.csrc.gov.cn/csrc/c101981/c2381308/content.shtml.

[2] The Cybersecurity Law, effective since 1 June 2017, is the first law addressing cybersecurity issues in China. See Cybersecurity Law of the People's Republic of China, available (in Chinese only) at http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[3] The DSL took effect from 1 September 2021. See Data Security Law of the People's Republic of China, available (in Chinese only) at http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml. Also See ICI Memorandum [33734], dated 23 August 2021, available at https://www.ici.org/memo33734.

[4] The PIPL took effect from 1 November 2021. See Personal Information Protection Law of the People's Republic of China, available (in Chinese only) at http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml. Also See ICI Memorandum [33738], dated 27 August 2021, available at https://www.ici.org/memo33738.

[5] The Draft Measures will apply to "Core Institutions," which refer to institutions that (i) undertake public functions in the securities and futures market, or (ii) operate information technology infrastructure in the securities and futures market. See Draft Measures, supra note 1, at Chapter 8, Article 62(1).

[6] Other securities and futures business Institutions include securities firms and futures companies. See Draft Measures, supra note 1, at Chapter 8, Article 62(2).

[7] Under MLPS, all network operators are required to assess the current state of their information and operations technology systems and the risks associated with them. They should propose a defined protection level for their network based on the potential impact of a data breach or system compromise. Levels range from 1 to 5, with 5 reserved for sensitive government facilities and systems. Higher levels have more stringent security requirements. Systems classified as Level 2 or above require an independent assessment by a recognized independent expert. Final certification will be issued by the region-level Public Security Bureaus.

[8] CIIs are defined as information infrastructure in the industries of public communication and information service, energy, transportation, water resources, finance, public service, e-government, national defense and military affairs and other important network facilities and information systems, the disruption, disfunction, and data leakage of which may endanger national security, civil livelihood, and public interest.

[9] The Draft Measures refer to the DSL for the definition of "core data" and "important data." See Draft Measures, supra note 1, at Chapter 8, Article 62(5).

"Core data" are data relevant to national security, the lifeline of the economy, important parts of people's livelihoods and major public interests. "Important data," on the other hand, is not defined under the DSL, but the DSL directs local governments and industry regulators to formulate their own categories of "important data" and measures to protect such data for their respective industries. See DSL, supra note 3, at Chapter 3, Article 21.

It is expected that, based on the general data classification framework stipulated under the DSL, the People's Bank of China / CSRC will issue industry-specific rules/requirements in relation to data classification for the financial industry.

[10] As defined in the PIPL, personal information refers to any information related to an identified or identifiable individual recorded whether electronically or through other means but does not include anonymized information. See PIPL, supra note 4, at Chapter 1, Article 4.
