LLINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

Shanghai
19F&16F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
Tel: +86 21 3135 8666
Fax: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

Beijing
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
Tel: +86 10 8519 2266
Fax: +86 10 8519 2929

香港
香港中环花园道 3 号
中国工商银行大厦 15 楼
电话：+852 2969 5300
传真：+852 2997 3385

Hong Kong
15F, ICBC Tower
3 Garden Road, Central
Hong Kong
Tel: +852 2969 5300
Fax: +852 2997 3385

www.llinkslaw.com
master@llinkslaw.com

Llinks Asset Management Bulletin
August 2017

Cybersecurity Law and WFOE PFM: Impact and Adaptive Strategies

By Sandra Lu, David Pan and Lily Luo

On 30 June 2016, Asset Management Association of China ("**AMAC**") released the *FAQs Regarding Registration and Record-Filing of Private Funds (No. 10)* ("**FAQ No. 10**") under the permission of China Securities Regulatory Commission ("**CSRC**"). *FAQ No. 10* allows foreign financial institutions to engage in private securities investment fund management business by establishing foreign-invested enterprises in the People' s Republic of China ("**China**" or "**PRC**"). A certain number of foreign financial institutions have been actively preparing to launch their wholly foreign-owned private securities investment fund management institutions ("**WFOE PFM**"). For instance, Fidelity and UBS have already completed their WFOEs' registration with AMAC to become WFOE PFMs and commenced their businesses accordingly.

Meanwhile, the impact of the *Cybersecurity Law of the People' s Republic of China* ("**Cybersecurity Law**" , effective as of 1 June 2017) and the subsequently issued or to-be-introduced complementary regulations and

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良：(86 21) 3135 8756
Publication@llinkslaw.com

If you would like other Llinks publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

guidelines thereunder on the businesses of WFOE PFMs should not be overlooked. Cybersecurity Law applies to any activity in relation to a network operator constructing, operating, maintaining or using the network. It provides the security operation regulations for network operators and requires the classified protection system for cybersecurity, the contingency plans and mechanisms for emergency disposal, the security and protection for the operation of critical information infrastructures ("**CII**"), the security assessment on the cross-border transfer of personal information and important data, etc. The question of how to balance between compliance with Cybersecurity Law and the need of fulfilling the corporate group' s compliance and risk control requirements, and sharing the group' s privileges and resources has become an issue to be considered and resolved by WFOE PFMs.

Investment and Trading Model of WFOE PFMs

FAQ No. 10 requires that a WFOE PFM "shall make investment decisions independently for securities and futures trading it deals with in Mainland China, and shall not place trading orders through any foreign institutions or foreign-based systems, except as otherwise stipulated by CSRC." Unlike a domestically-invested private fund manager, a WFOE PFM should take into consideration the requirement of legal compliance and risk control on a corporate group level in order to comply with both domestic and foreign laws and regulatory requirements, such as those regarding the KYC (know your clients), anti-money laundering, risk control of investment and trading, disclosure of interests. On the other hand, the WFOE PFMs also wish to share the existing advantages and resources of the corporate group (such as researches in securities, quantitative models and risk control systems). Having regard to the concern and needs of a WFOE PFM, the FIX[1] model, which applies to WFOE PFMs, is proposed by some foreign institutions.

Specifically, a responsible officer for making investment decisions and a responsible officer for placing trading orders should be equipped with by a WFOE PFM. If FIX model is adopted, a terminal of the global investment management and trading system of the corporate group should be installed in China, and the terminal can connect the PRC securities brokers through the FIX connectivity. After the WFOE PFM' s portfolio manager makes a preliminary investment decision, such decision may be submitted to the global investment management and trading system for compliance and risk control review, and then the final investment decision shall be made by the WFOE PFM' s portfolio manager based on the results of the review. The trader of

WFOE PFM places trading orders with the PRC securities brokers through the FIX connectivity (or telephone, e-mail, fax and/or other communication methods), ensuring that the trade routes are transparent and traceable, the trade data is complete and identifiable, the trading process is clear and controllable, and the trade records are all traceable and backed up in China.

The FIX model inevitably involves the storage of investment and trading data outside China and the cross-border transfer of data. Apart from that, in order to satisfy the compliance and risk control requirements on a corporate group level, such as KYC and anti-money laundering, a WFOE PFM has to input the client' s information into the corporate group' s system, which also involves the cross-border transfer of client information.

Impact of Cybersecurity Law on WFOE PFMs

1. Major Provisions of Cybersecurity Law

Cybersecurity Law and the Complementary Provisions and Guidelines

Articles of Cybersecurity Law	Complementary Provisions/Guidelines
Formulating the security review measures for network products and services (Article 15, Article 22)	*Interim Measures for Security Review on Network Products and Services* (effective as of 1 June 2017)
Formulating the classified protection system for cybersecurity (Article 21)	To be introduced
Formulating the catalogue for critical network equipment and specialized cybersecurity products (Article 23)	Announcement Regarding the Issuance of the *Catalogue for Critical Network Equipment and Specialized Cybersecurity Products (First Batch)* (published on 1 June 2017) [2]
Formulating the specific scope and measures for security and protection of CII (Article 31)	*Regulations on the Security and Protection of Critical Information Infrastructures (Draft for Consultation)* (issued on 10 July 2017)

Cybersecurity Law and WFOE PFM:

Impact and Adaptive Strategies

LINKS Law Offices 通力律师事务所

Articles of Cybersecurity Law	Complementary Provisions/Guidelines
Formulating the CII identification guidelines (Article 31)	To be introduced Cyberspace Administration of China will take lead and work together with the Ministry of Industry and Information Technology of the People's Republic of China, the Ministry of Public Security of the People's Republic of China and other departments to formulate specific CII identification guidelines. The national competent industry authorities or the regulators shall organize and identify the CII of this industry and field in accordance with the CII identification guidelines, and report the identification results according to the relevant procedures.
Formulating measures for the security assessment on cross-border transfer of personal information and important data (Article 37)	*Measures for the Security Assessment on Cross-border Transfer of Personal Information and Important Data (Draft for Consultation)* (issued on 11 April 2017), and the *Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Amended Draft)* formulated in May 2017 (not yet published)
Formulating national standards – security regulations for personal information	*Information Security Techniques - Personal Information Security Specification (Draft for Consultation)* (issued on 20 December 2016)
Formulating national standards – guidelines for security assessment on cross-border transfer of data	*Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft)* (issued on 27 May 2017)

Definitions Closely Related to WFOE PFMs under Cybersecurity Law

"Network" refers to the system that is constituted by computers or other information terminals and relevant equipment to collect, save, transmit, exchange, and process information pursuant to certain rules and procedures. The WFOE PFM' s investment management and trading system and other network systems, as well as websites fall into the scope of "Network" .

"Network operators" refer to owners and/or administrators of the network and network service providers. WFOE PFMs, if they own and/or administrate networks, are network operators.

"Critical information infrastructure/CII" refers to critical information infrastructures of important industries and fields, such as public communication and information services, power, transportation, water conservancy, finance, public services, and e-government affairs, as well as other infrastructures that might seriously endanger national security, national economy, people' s livelihood, or public interests in the event of damage, malfunctioning, or data leakage. Emphasized protection is given to CII in addition to the basic classified protection system for cybersecurity.

"Personal information" refers to all kinds of information recorded by electronic methods or otherwise, which can be used independently or in combination with other information to identify a natural person' s identity. Such information includes but is not limited to a natural person' s name, date of birth, ID number, biologically identified personal information, address and telephone number.

"Important data" , with reference to the *Measures for the Security Assessment on Cross-border Transfer of Personal Information and Important Data (Draft for Consultation)*, refers to data closely related to national security, economic development and societal or public interests. The specific scope of "important data" is illustrated in the relevant national standards and the identification guidelines for important data. Appendix A of the *Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft)*, a national standard drafted by the National Information Security Standardization Technical Committee, provides the scope of important data.

"Cross-border transfer of data" , with reference to the *Measures for the Security Assessment on Cross-border Transfer of Personal Information and Important Data (Draft for Consultation)*,

means the provision of personal information and important data collected or generated in the course of operation in the PRC by network operators to institutions, organizations or individuals located overseas.

Major Content of Cybersecurity Law Applicable to WFOE PFM

(1) Scope of application: Cybersecurity Law applies to the construction, operation, maintenance and use of network as well as the supervision and administration of cybersecurity within the territory of the PRC. The investment management and trading system used by WFOE PFMs falls under "network" as defined by Cybersecurity Law. Even the server of the global investment management and trading system used by a WFOE PFM under FIX model is located offshore, as the WFOE PFM uses such system within the territory of the PRC, it is our understanding that the usage of the system should be subject to Cybersecurity Law. (Article 2 of Cybersecurity Law)

(2) Classified protection system for cybersecurity: Cybersecurity Law proposes a "classified protection system for cybersecurity" . Network operators shall fulfill security and protection obligations in accordance with the requirements of the classified protection system for cybersecurity. Such obligations include: formulating internal security management systems and operating instructions, determining the persons responsible for cybersecurity and implementing the cybersecurity and protection responsibilities; taking technical measures to prevent computer viruses, network attacks, network intrusions and other acts endangering cybersecurity; taking technical measures to monitor and record the network operation status and cybersecurity incidents, and preserving web logs for no less than six months pursuant to the provisions; taking measures such as data classification, back-up and encryption of important data, etc. (Article 21 of Cybersecurity Law)

(3) Network operators shall formulate contingency plans for cybersecurity incidents and carry out such activities as cybersecurity authentication, inspection and risk evaluation. (Articles 25 and 26 of Cybersecurity Law)

(4) CII: Regulated according to the provisions of Chapter III of Cybersecurity Law on the scope of CII, including but not limited to more stringent security and protection obligations, security review and execution of security confidentiality agreements for purchases of network products and services, onshore storage of personal information and important data

collected and generated in the course of operation within the territory of the PRC by CII operators and security assessment where it is necessary to provide such personal information and important data to overseas parties, and annual inspection and assessment. (Articles 31, 34, 35, 36, 37 and 38 of Cybersecurity Law)

(5) Protection of personal information: To collect and use personal information, network operators shall express the purposes, means and scope of collecting and using the information towards the subject of information, and obtain the consent therefrom. Network operators shall not divulge, distort or damage the personal information collected; and shall not provide the personal information to others without the consent of the persons whose data is collected. The above rules do not apply where the information has been processed and cannot be recovered, which makes it impossible to match such information with specific persons. (Articles 41 and 42 of Cybersecurity Law)

(6) Legal liability: Chapter VI of Cybersecurity Law clearly provides the legal liabilities of network operators in the event of breach of their relevant responsibilities and obligations, such liabilities include being ordered to effect rectification, being warned, being fined, being ordered to suspend relevant business, stop business for rectification, close down website(s), having the relevant business permits or licenses revoked, having the personnel directly in charge fined, etc.

2. WFOE PFM and CII

Cybersecurity Law and the Regulations on the Security and Protection of Critical Information Infrastructures (Draft for Consultation) define CII by listing examples and summarizing consequences where cybersecurity incidents occur in relation to the CII. Among the listed examples, "finance" is the most relevant industry and field regarding WFOE PFMs, as for the consequences, CII is shown to be a highly important network for national security, national economy, people' s livelihood and social stability.

To date, there is yet to be a conclusion on whether a private fund management institution is a financial institution or not. According to *Coding Standards for Financial Institutions* (JR/T 0124-2014) issued by the People' s Bank of China on 19 September 2014, "securities investment fund management companies" refer to legal corporations established within the

territory of the PRC under the approval of CSRC, which conduct securities investment fund management business. As WFOE PFMs complete private fund manager registration with AMAC in order to commence their private fund management business, it seems unlikely that they should fall within financial institutions covered by the *Coding Standards for Financial Institutions* issued by the People' s Bank of China. According to the *National Standard Industrial Classification of National Economy* (GB/T 4754-2011), "financial sector - capital market services - fund management services" (code: 6713) refers to the asset portfolio and fund management activities carried out for individuals, corporations and other clients on the basis of remuneration or a contract, which include securities investment fund, enterprise annuity, social security fund, segregated account management, management of outbound investments by domestic capital (QDII), etc. Pursuant to this definition, private securities investment fund management business may fall within the realm of "financial sector" .

It is necessary to point out that not all the network infrastructures and information systems operated and managed by an institution that falls within the scope of critical sectors are CII. It is also important to take into account the extensiveness of the support provided by the network infrastructure or information system to the critical sectors and the consequences and level of danger in the event of cybersecurity incidents in order to judge whether such infrastructure or system is a CII or not. The question of whether the investment management and trading system of the WFOE PFMs and other core information systems are recognized as CII still begs further analysis which could be done after the introduction of the pending *CII Identification Guidelines*.

If the investment management and trading system or other core information systems used by WFOE PFMs are recognized as CII, WFOE PFMs as CII operators will have more onerous responsibilities and obligations than those for general network operators, according to Cybersecurity Law and the *Regulations on the Security and Protection of Critical Information Infrastructures (Draft for Consultation)*. Specifically, such responsibilities and obligations include:

(1) The person in charge of the WFOE PFM should be the first responsible person for the security and protection work of the CII, and the cybersecurity management department should be set up and the key personnel for cybersecurity management should be designated, and security background check should be conducted on the responsible officer and the personnel assuming other key positions;

(2) Regularly conducting cybersecurity education, technical training and skill assessment for the practitioners;

(3) Implementing disaster recovery back-ups for important systems and databases, promptly taking remedial measures for system vulnerabilities and other such security risks;

(4) Formulating contingency plans for cybersecurity incidents and conduct regular rehearsals for tackling cybersecurity incidents;

(5) Establishing a comprehensive CII security inspection and assessment system as well as carrying out such inspection and assessment at least once a year;

(6) **Storing within the PRC the personal information and important data** collected and generated in the course of operation within the territory of the PRC. **Where, for business needs, it is necessary to provide such personal information and important data to overseas parties, assessment should be conducted on such cross-border transfer of data in accordance with the measures for security assessment on cross-border transfer of personal information and important data;**

(7) **Implementing the operation and maintenance of CII within the PRC**. Where, for business needs, it is necessary to carry out overseas distant maintenance, such circumstance should first be reported to the national competent authorities or regulators and the public security authority of the State Council;

(8) **Guaranteeing that purchases and uses of critical network equipment and specialized cybersecurity products should be in compliance with the laws, administrative regulations and the compulsory requirements imposed by the relevant national standards** and pass the cybersecurity review, and also entering into security confidentiality agreements with the providers.

The responsibilities and obligations listed in items (6), (7) and (8) above have a crucial impact on whether the use of FIX model by WFOE PFMs may be continuously feasible. If the investment management and trading system of a WFOE PFM belongs to CII, and client information and investment trading data belong to "important data" , the compulsory requirements of items (6), (7) and (8) above may impair the applicability of FIX model by WFOE

PFMs, and that WFOE PFMs would either have to purchase investment and trading systems onshore which comply with the requirements, or rearrange the global investment management and trading system to be localized according to the requirements stipulated by the laws and regulations. WFOE PFMs may pay closer attention to the upcoming official versions of the *CII Identification Guidelines and the Regulations on the Security and Protection of Critical Information Infrastructure*s to ensure good compliance preparation.

3. WFOE PFM and "Important Data"

Although Cybersecurity Law has only mentioned the requirements that the CII operators should store personal information and important data within the PRC and conduct security assessment where it is necessary to provide such data to overseas parties, other than Cybersecurity Law, the high-level laws of the *Measures for the Security Assessment on Cross-border Transfer of Personal Information and Important Data also include the National Security Law of the People' s Republic of China*. This means that "important data" which is needed to be stored within the PRC and whose cross-border transfer should not be conducted without security assessment also include important data collected and generated within the PRC by general network operators, and not only limited to those collected and generated within the PRC by CII operators.

Referring to Appendix A - A.19 of the *Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft)*, important data of finance and fields related to the financial industry includes but without limitation to:

A.19.1 Security Information of Financial Institutions

a) Research and development plans of new products and the relevant records and data generated in the course of research and development;

b) Technical plans, circuit designs, computer software, source codes and target codes, databases, research and development records, technical reports, inspection reports, experimental data, experimental results, drawings and other technical documents;

c) Product sales information, market research information, marketing plans, financial information, business analyses, research results and other such operation information;

d) Client name list, client identity information, client trade records and other such client information;

e) Internal security system, operational details, the test key used for banking business, formulated plans and special secret marks, codes, and command passwords;

f) Other information which would cause damage to the security and interests of the financial institutions if it is leaked.

A.19.2 Financial Information of Natural Persons, Legal Persons and Other Organizations

a) Individual financial information, including an individual' s income status, status of immovable property in his/her possession, status of vehicles in his/her possession, amount of tax payable, provident fund deposit amount, etc.;

b) Account information, including information of bank settlement accounts and payment accounts. The major information consists of: account name, account number, account type, account opening date, account opening institution, information of bound accounts, account verification information (including information of client identity verification conducted through external channels), information of sensitive media as reflected by the account (such as valid period of the bank card, verification code, magnetic stripe information), account balance, account transactions, etc.

c) Personal credit information, including credit card repayment status, loan repayment status and other information formed by an individual' s economic activities which may reflect the individual' s credit status;

d) **Information on financial transactions of natural persons, legal persons and other organizations, including trading information of natural persons, legal persons and other organizations obtained in the course of business by financial institutions of the banking industry, securities industry, insurance industry, financial institutions dealing with trades and settlement, non-bank payment institutions and other financial institutions;**

e) **Identity information, including personal identity information and the identity information of an institution**. Personal identity information includes the individual' s name, gender, nationality, ethnicity, type and number and valid period of the identity card, occupation, contact method, marriage status, family status, residential or office address and photos, etc. Identity information of an institution includes the name of the institution, the unified social credit code and type, name and identity certificate number of the legal representative (responsible person), business premise, contact method, etc.;

f) Derived information, including personal consumption habits, investment will and other such information derived from the processing or analyzing of original information, which reflects certain aspects of specific persons;

g) Other information of natural persons, legal persons and organizations obtained and kept in the course of building business relationships with them.

It could be seen from the above that a WFOE PFM should not only pay attention to issues regarding CII explained in point 2 as above, but in relation to "important data" which has to be stored and reviewed for cross-border transfer for security purpose, a WFOE PFM also has to pay attention to the scope of obligors thereof and the scope of "important data" which will be stipulated respectively in the final effective versions of the *Measures for the Security Assessment on Cross-border Transfer of Data* and the *Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment*. Even if WFOE PFMs are eventually not classified as CII operators, it is still possible that they would have to abide strictly by the rules set out in the *Measures for the Security Assessment on Cross-border Transfer of Data* because the information they collect may fall within the scope of "important data" .

4. Security Assessment on Cross-border Transfer of "Personal Information" and "Important Data"

According to the *Measures for the Security Assessment on Cross-border Transfer of Data (Draft for Consultation)*, WFOE PFMs, as network operators, shall conduct security assessment on the cross-border transfer of personal information and important data collected and generated in the course of operation in the PRC. In general, WFOE PFMs may refer only to the requirements set

out in the relevant regulations and guidelines to formulate and implement internal measures for security assessment, and the cross-border transfer of personal information also requires the obtainment of prior consent of the information subject. However, in the event of the following circumstances, WFOE PFMs should report to and request the regulator (CSRC) to organize a security assessment:

(1) Where the personal information of over 500,000 individuals is contained or aggregated;

(2) Where the volume of data exceeds 1,000 GB; *(removed by the Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Amended Draft))*

(3) Where data in the fields of nuclear facilities, chemistry and biology, national defense and the military, population health, or data on megaproject activities, data on marine environment or sensitive geographic information, etc., is involved;

(4) Where cybersecurity information of CII, such as system vulnerabilities, security and protection, is involved;

(5) Where it involves the cross-border transfer of personal information and important data by a CII operator; *(removed by the Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Amended Draft))* [3]

(6) Where the national security and the societal or public interests may otherwise be affected, and the competent authorities and the regulators deem necessary to assess such transmission of data.

Overview of CII in the U.S. and EU countries and Possible References China Can Make

1. Relevant System under the U.S. Law

There is no such thing named as "critical information infrastructure" under the U.S. law; rather, the subject is defined as an information system used to support a critical infrastructure. "Critical

infrastructure" usually refers to any system or infrastructure that plays a critical role in relation to national security and the normal operation system of the society. In 2002, the U.S. passed the *Homeland Security Act*, and the Department of Homeland Security became the competent department of critical infrastructure, resulting in a close connection between critical infrastructure and homeland security. The *Critical Infrastructures Protection Act of 2001* provides that, "critical infrastructures means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [4]

In 2003 and 2008, the sectors and fields covered by critical infrastructures varied, until 2013, the Presidential Policy Directive No. 21 [5] eventually confirmed 16 critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, **financial services**, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, water and wastewater systems. On 11 May 2017, President Trump signed off a presidential executive order, demanding the strengthening of cybersecurity of federal critical infrastructures [6].

The Department of Homeland Security designated a sector-specific agency responsible for cybersecurity of each critical infrastructure. According to the sector guidelines issued by the Department of Homeland Security, financial services sector is inclusive of "invest funds for both long and short periods" , and the competent department in charge of cybersecurity of the financial services sector is the U.S. Department of the Treasury. According to Financial Services Sector-Specific Plan 2015, the Financial Services Sector Coordinating Council, which is made up of the major institutions of the financial sector, assisted the Department of Homeland Security to pass projects such as "information sharing" , "best practices" , "incident response and recovery" and "policy support" , to facilitate the cybersecurity of critical infrastructures of the financial services sector [7].

2. Relevant System under the EU Law

The *Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection* [8] issued in 2008 provides that critical infrastructure shall refer to an asset, system or part thereof located in Member States

which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions. The Member States of the EU generally consider "finance" as within the scope of critical infrastructures.

Specifically regarding critical infrastructures, the European Union Agency for Network and Information Security ("**ENISA**") advocates the implementation of the national strategy of information protection for the national network, under which the specific measures are similar to China' s CII operator administrative system. For instance, there are measures for the formulation of contingency plans for cybersecurity incidents, the organization of cybersecurity rehearsals, the formulation of the basic standards of cybersecurity, the setting up of a report mechanism for cybersecurity incidents and the reaction capacity towards such incidents.

It is especially worth noting that, the many years of experience of the EU shows that it is important to balance public and private interests in the security administration of CII. ENISA' s report points out that, "Information-sharing among private and public stakeholders is a powerful mechanism to better understand a constantly changing environment. Information-sharing is a form of strategic partnership among key public and private stakeholders. Owners of critical infrastructures could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of national security, including findings based on information collected by intelligence and cyber-crime units." For the sake of balancing public and private interests, the EU specifically stressed that "a public-private partnership (PPP) establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals " [9].

Analysis on Adaptive Strategies of WFOE PFMs

As regulations on cybersecurity have already ascended to a level concerning "state sovereignty in space" , how a WFOE PFM should commence its business in compliance with Cybersecurity Law has become a serious problem which cannot be neglected. We hereby provide a few suggestions on the adaptive strategies that a WFOE PFM may take at the present stage:

1. Paying close attention to the legislation progress of the complementary regulations and guidelines of Cybersecurity Law and the corresponding arrangements of transition period;

2. Being well-prepared to satisfy compliance requirements. For example, based on the existing regulations and the relevant consultation papers, to draft a cybersecurity protection system, contingency plans and emergency disposal mechanisms, system and procedures of security assessment on the cross-border transfer of personal information and important data, and to reorganize the collection procedures of personal information;

3. Maintaining communication with the Cyberspace Administration of China, CSRC and AMAC. Apart from paying close attention to the legislation progress, WFOE PFMs may also actively provide suggestions towards those authorities, such as:

(1) Regarding the CII Identification Guidelines, the experiences of the U.S. and the EU may be referred to, e.g. public-private partnership may be promoted to realize the balance between public and private interests; the self-disciplinary authority of the industry (AMAC) may formulate corresponding rules in accordance with the characteristics of private fund industry by taking into consideration the industry nature (whether a WFOE PFM is a financial institution and whether the PFM business belongs to financial industry), the importance of the system (whether the system is a core business system), whether the operator has owned a certain number of clients, a certain amount of data, and a certain scale of assets under management. Such an approach may realize a dynamic supervision and regulation and make compliance with laws and regulations become more predictable, so that a WFOE PFM can be well prepared to satisfy compliance requirements;

(2) Whether it is possible to exempt or simplify the procedures of security assessment over cross-border transfer of personal information and important data on an intra-group basis for the purpose of compliance and risk control;

(3) In the event that circumstances invoking the organization of a security assessment by the regulator occur, the regulator may take into account the need of real-time trades of the fund management business and other such characteristics to conduct regular assessment, instead of conducting an assessment every time data is transmitted outbound;

(4) If WFOE PFMs belong to CII operators and that investment management and trading system falls within the definition of CII, whether it is possible that a longer transition period could be provided to WFOE PFMs which have adopted FIX model, so that the relevant WFOE PFMs may localize the global investment management and trading system, or purchase a local investment trading system and upgrade it to satisfy the compliance and risk control requirements set out by the group corporate.

【Note】

[1] FIX refers to Financial Information eXchange, which is a digital trade orders transmission agreement commonly used around the world. It may be understood as a unified "language" for information transmission. FIX connectivity is commonly selected and used by the buyers, sellers, trade platforms, securities regulatory authorities and stock exchanges around the world, thus, the use thereof has become a global trading practice. The global investment management and trading systems of the corporate groups usually support FIX connectivity. Moreover, FIX connectivity is also commonly used in QFII/RQFII business and Stock Connect business, and the execution systems of most of domestic securities companies can support FIX connectivity.

[2] See details of the *Catalogue*: http: //www.cac.gov.cn/2017-06/09/c_1121113591.htm

[3] Article 37 of Cybersecurity Law clearly provides the obligations of CII operators to store within the PRC "personal information" and "important data" and conduct security review on cross-border transfer of such data. Hence, the removal of this item by the *Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Amended Draft)* does not affect the obligations of CII operators under Article 37 of Cybersecurity Law.

[4] *Critical Infrastructures Protection Act of 2001*, https: //www.congress.gov/bill/107th-congress/senate-bill/1407/text?q=%7B%22search%22%3A%5B%22critical+infrastructure+protection+act%22%5D%7D&r=4

[5] Presidential Policy Directive No. 21 released in 2013 – Critical Infrastructure Security and Resilience, https: //obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] https: //www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

[7] https: //www.dhs.gov/financial-services-sector

[8] 8 December 2008, 2008/114/EC, *Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*, http: //eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: L: 2008: 345: 0075: 0082: EN: PDF

[9] European Union Agency for Network and Information Security, Report on *National Cybersecurity Strategies - Practical Guide on Development and Execution*, http: //www.gisti-thinkbank.ac.cn/admin/upload/20131113-20130823.pdf

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Sandra Lu Tel: (86 21) 3135 8776 sandra.lu@llinkslaw.com	**David Pan** Tel: (86 21) 3135 8701 david.pan@llinkslaw.com
Lily Luo Tel: (86 21) 3135 8732 lily.luo@llinkslaw.com	
Shanghai	
Christophe Han Tel: (86 21) 3135 8766 christophe.han@llinkslaw.com	**Charles Qin** Tel: (86 21) 3135 8668 charles.qin@llinkslaw.com
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: (86 21) 3135 8776 sandra.lu@llinkslaw.com
Nicholas Lou Tel: (86 21) 3135 8766 nicholas.lou@llinkslaw.com	**Tommy Xia** Tel: (86 21) 3135 8769 tomy.xia@llinkslaw.com
Raymond Li Tel: (86 21) 3135 8663 raymond.li@llinkslaw.com	**Elva Yu** Tel: (86 21) 3135 8793 elva.yu@llinkslaw.com
Desmond An Tel: (86 21) 3135 8725 desmond.an@llinkslaw.com	
Beijing	
Leo Wang Tel: (86 10) 3135 8716 leo.wang@llinkslaw.com	**Monica Gao** Tel: (86 10) 8519 1625 monica.gao@llinkslaw.com
Hong Kong (in Association with Vivien Teu & Co LLP)	
David Yu Tel: (86 21) 3135 8686 david.yu@llinkslaw.com	**Sandra Lu** Tel: (86 21) 3135 8776 sandra.lu@llinkslaw.com