China Newsletter Spring 2020 Direct Investment & Compliance

Article By
China Law Practice Group
Greenberg Traurig, LLP
GT China Newsletter

- Administrative & Regulatory
- Biotech, Food, Drug
- Communications, Media & Internet
- Financial Institutions & Banking
- Intellectual Property
- China

Monday, June 8, 2020

China’s Implementation Rules for Foreign Investment Law

On Dec. 26, 2019, the State Council released the Implementing Regulations of the Foreign Investment Law (the Implementing Regulations), which took effect Jan. 1, 2020. The Ministry of Justice, Ministry of Commerce, and National Development and Reform Commission jointly remarked at a press conference that the Implementing Regulations facilitate the Foreign Investment Law in five ways: (1) the national supportive policies are equally applicable to foreign-invested enterprises; (2) they improve the transparency of policies related to foreign investment in China (including collection of comments and suggestion, timely release of policies); (3) they encourage and provide guidance for foreign investment with clear policies and preferential treatment; (4) they ensure the equal involvement of foreign investors in developing and revising national, industrial, local, and group standards; (5) they ensure equal involvement of foreign investors in Chinese government procurement.

1. Strengthened Enforceability and Validity of Investment Agreements with Chinese Government

For any foreign investment agreement involving different levels of the Chinese
government, in particular for greenfield projects, foreign investors are highly motivated by advantageous treatment and incentives (e.g., access to land and facilities, tax benefits) when deciding to make an investment and/or entering into such investment agreement with the Chinese government. In the past, the government authorities sometimes dishonored their commitments, and the investors were reluctant to resort to legal proceedings for the enforcement of the agreements. Because the investors prioritized having a good relationship with local government authorities, they often remained silent as to their loss. The Implementing Regulations provide a clear basis for foreign investors to hold the Chinese government accountable for its promises and commitments, by expressly disallowing the government’s use of excuses (such as changes to the head of local government or government divisions, and the reshuffling of the functions of the government body), for backing out of its contractual obligations.

Further, the Implementing Regulations provide that if the government body or any relevant staff fail to comply with their policy commitment or signed agreements, or the policy commitment made is beyond their legal authority or is illegal, such government body and relevant staff will assume legal liabilities “in accordance with laws and regulations.” Although the warning is directed to the government authority and relevant staff, the vague reference to legal liability may be mere posturing. The Implementing Regulations draw no clear distinction between the contracts made within the government’s statutory authority (or according to law) and those made beyond such authority (or not according to law). Thus, it remains to be seen whether such requirement will be enforced if the government fails to follow its contractual obligations.

2. Changes to Government Functions and Industrial Restrictions

As neither the Foreign Investment Law nor the Implementing Regulations have given the Ministry of Commerce authority to review the eligibility of related permissions for foreign investment (which is provided in the Negative List, see GT’s Winter 2019 China Newsletter for details on the Negative List) and review the related commercial agreements, the Ministry of Commerce no longer functions as the “front office” regulating foreign investment. Previously, the departments of the Ministry of Commerce would request the revision of commercial agreements made between a Chinese party and a foreign party. The Implementing Regulations formally remove the Ministry of Commerce from the “front office,” marking the end an era.

Although Article 35 of the Implementing Regulations provides that competent industry authorities should review applications for industrial licenses of foreign investors based on equal treatment for domestic companies and foreign-invested companies, various restrictive measures remain imbedded in regulations for different industries (e.g., the Provisions on Foreign Investment in Civil Aviation Industry and the Administrative Provisions on Foreign-Invested Telecommunications Enterprises). Such regulations (which are still in effect) set some restrictive conditions regarding shareholding ratio and shareholder qualification (including record of good performance and operating experience in related business). Foreign investors should pay attention to the regulations for their particular industries, though legislative work abolishing and revising such regulations (which contradict the equal protection for domestic investment and foreign investment set by
the *Foreign Investment Law* and the *Implementing Regulations*) is in progress.

3. Intellectual Property Rights Protection

Article 24 of the *Implementing Regulations* provides that no administrative authority or officials may force any foreign investor or foreign-invested enterprise to transfer its technology by virtue of implementing administrative licensing, administrative inspection, administrative punishment, administrative enforcement, or other administrative means. “Administrative means” is thereby broadened by the *Implementing Regulations* as to what is forbidden in forcing a transfer of technology stipulated in Article 22 of the *Foreign Investment Law*. After the release of the *Foreign Investment Law*, the State Council revised the *Administrative Regulations on Technology Import and Export* by deleting the original Article 29 (which forbids the restrictive clauses in a technology import contract, such as restricting the receiving party from improving the technology supplied or restricting the receiving party from obtaining technology similar to that supplied technology). Such revision may help improve the protection for intellectual property rights, and ensure the technology transfer will be conducted based on principle of voluntary equality.

4. Five-Year Grace Period

The *Foreign Investment Law* sets a five-year grace period (starting Jan. 1, 2020) for foreign-invested enterprises to adapt to the new legal framework, to create the required organizational form and organizational structure. The *Implementing Regulations* provide that upon expiration of the five-year grace period (starting Jan. 1, 2025), the foreign-invested enterprises that have not adjusted their organizational form and organizational structures will not be permitted to formally change registration. Further, the competent market regulatory authority will publicize the relevant situation of such non-compliant enterprises and will not execute the enterprises’ other registration matters.

Some foreign-invested enterprises note that the abolished legal framework (the *Sino-Foreign Equity Joint Ventures Law*, the *Wholly Foreign-Owned Enterprises Law*, the *Sino-Foreign Cooperative Joint Ventures Law*) provided a preferential system for distribution on dissolution and dividends of cooperative enterprises, from which more flexibility could be enjoyed by foreign-invested enterprises. Article 46 of the *Implementing Regulations* allows for the continuation of such flexibility (including measures for shareholdings or equity transfer, earning distribution and residual property distribution, etc.), which, as provided in the relevant contract by the parties (concerning the original equity or cooperative joint venture), may survive even after the organizational form and organizational structure of an existing foreign-invested enterprise is legally adjusted.

5. Matters to be Clarified

- New Project: the *Foreign Investment Law* lists “a new project” (initiated within the territory of China by a foreign investor, independently or jointly with any other investor) as one form of foreign investment, and the *Draft for Comments of the Implementing Regulations* defined such “new project” as “foreign investors investing in the forming/construction of specific projects within the territory of China, but without establishing foreign-invested enterprises, or acquiring
shares, equity, property shares or other similar rights and interests.” However, the Implementing Regulations omit this definition for “new project,” so it remains to be clarified in later legislation and practice.

- Application of law: While the abolished legal framework for foreign-invested enterprises required the application of Chinese law, the new legal framework does not require such application. However, as foreign-invested enterprises are established and operated in China, such strong connection may lead to application of Chinese law.

Facilitating Cross-Border Investment: Non-Investment FIEs May Re-Invest with Capital Fund in China

On Oct. 23, 2019, State Administration of Foreign Exchange (SAFE) issued the Circular on Further Promoting Cross-border Trade and Investment Facilitation (Circular 28), introducing a series of measures to facilitate cross-border trade and investment. Loosening the restriction on re-investment by non-investment foreign-invested enterprises (FIE) with their capital funds is the highlight of Circular 28.

Since 2008, SAFE has issued several circulars to address its policy on re-investment with capital funds. The consistent rule has generally been a prohibition on re-investment by FIEs with capital funds, except that foreign-invested investment companies may re-invest with capital funds. However, it is difficult for foreign investors to satisfy the threshold of an investment company under Chinese law. Among the 370,000 FIEs registered in China, only 3,000 of them are investment companies, accounting for 1%.

Under Circular 28, non-investment FIEs may re-invest with capital funds as long as the following two conditions are satisfied:

- The re-investment shall not violate the restrictions and prohibitions under the Negative List. Circular 28 does not change the market access system under Negative List.
- The re-investment shall meet the requirement of authenticity and compliance. Such requirement may pose some barriers to re-investment. Earlier practice in pilot areas shows that banks may insist that the re-investment and the business of the target company is to some extent related to the current business of the FIE, and banks may turn down a re-investment project not related to the current business due to concern of speculative investment.

Using a real estate group as an example, before Circular 28, a foreign real estate company had to directly control separate project companies in China with an overseas entity, rather than establish a holding company in China, if it failed to establish a qualified investment company. This was because a non-investment company was prohibited from re-investment with capital funds. Circular 28 allows
such foreign company, taking tax benefits into consideration, to establish a local holding company in China to manage various project companies.

**NMPA Releases Drafts for Review of Measures Related to the Registration, Production and Operation of Drugs**

To promote the implementation of the *Drug Administration Law* and further clarify the updated requirements for drug administration, the National Medical Products Administration (NMPA) released on Dec. 10, 2019, the latest versions of *Administrative Measures for Drug Registration (Draft for Comment)* (the *Registration Measures*), the *Measures for the Supervision and Administration of Drug Production (Draft for Comment)* (the *Production Measures*) and the *Measures for the Supervision and Administration of Drug Operation (Draft for Comment)* (the *Operation Measures*) for public comment.

The major changes of the *Production Measures* and the *Operation Measures* correspond with the revisions to the *Drug Administration Law*, including the application of the Marketing Authorization Holder System (MAH System). In terms of drug production, regardless of whether the MAH produces drugs by itself, it shall be responsible for the quality of drugs throughout the whole of production, control, release, storage and transport, to ensure safety, efficacy and quality control. Where the MAH does not complete drug production on its own, it shall sign an entrustment agreement and a quality agreement with the qualified drug production enterprise, and the entrusted party is prohibited from sub-contracting with any third party to produce the drugs. As for drug operation, MAHs shall establish the drug quality assurance system when selling drugs, to fulfill their responsibilities of quality management in the whole process of drug operation. Where an MAH contracts with a drug distributor to sell drugs, it shall enter into an entrustment agreement with the entrusted party to specify responsibilities for drug quality, and the MAH shall supervise the entrusted party.

The *Registration Measures* reflect the updated the *Drug Administration Law* in various aspects, including the modification and re-registration of post-marketing drugs, and the supervision and inspection of drug research institutions and drug clinical trial institutions, to ensure that the administration of drug registration will run through the whole life cycle of drugs. In addition, the *Registration Measures* stipulate the channels of accelerated marketing registration of drugs, including breakthrough therapeutic drugs, conditional approval, priority review and approval, special examination and approval, along with the applicable scope, application procedures, supporting policies, and termination procedures of each channel. The *Registration Measures* also include drugs in short supply, drugs used by children, drugs for rare diseases, highly innovative drugs, and vaccines urgently needed for disease prevention and control as listed in the *Drug Administration Law*, the *Vaccine Administration Law*, and relevant documents issued by the State Council relating to accelerated marketing registration.

In addition, the *Registration Measures* improves existing drug registration
procedures: (i) the time limit for review of a marketing registration application for a
drug is limited to 200 working days; (ii) competent authorities must classify the
modes of on-site inspection of drug registration based on the degree of product
innovation and risks, and shall conduct both on-site inspection of drug registration
and Good Manufacturing Practice (GMP) inspection prior to marketing of drugs; and
(iii) the Registration Measures clearly provide that, where there is any change in the
sponsor of a drug clinical trial, the post-change sponsor shall undertake the
responsibilities and obligations relating to drug clinical trials.

New Cryptography Law Reshapes Commercial Encryption Standards

On Jan. 1, 2020, the Cryptography Law of the People's Republic of
China (the Cryptography Law) came into effect. The Cryptography Law follows the
general principle of reducing market access barriers to commercial cryptography.
While it is closely aligned with cybersecurity law, additional regulatory
requirements in the Cryptography Law may make it more difficult for companies to
come into compliance. The Cryptography Law also emphasizes the principle of non-
discrimination against foreign-invested enterprises and prohibits compulsory
technology transfer.

1. Classification of Cryptography

Cryptography under the Cryptography Law refers to technologies, products, and
services applying specific transformation methods to information to effect
encryption protection or security authentication.

The Cryptography Law divides cryptography into three categories:

- Core cryptography: used to protect state secret information with a highest
  secret level of top secret;
- Ordinary cryptography: used to protect state secret information with a highest
  level of secret; and
- Commercial cryptography: used to protect secret information that does not
  constitute state secrets.

2. Reducing Market Access Barriers to Commercial Cryptography

In 2017, the State Council repealed four administrative licenses under Regulation of
Commercial Encryption Codes, including the license of manufacturers of commercial
cryptography products, license of sellers of commercial cryptography products,
license of use of foreign-made cryptography products by foreign-invested
enterprises, and use of cryptography products by foreign organizations and
individuals. The Cryptography Law has formally and legally cancelled these licenses.

However, the State Cryptography Administration retains the following
licenses/requirements:

- producers and sellers of commercial cryptography products are required to acquire certificates of commercial cryptography products models;

- foreign invested enterprises, foreign organizations, and foreign individuals are required to acquire importation licenses for using imported cryptography products; and

- enterprises with certificates of commercial cryptography products models are required to file with local cryptography administrations for annual sales figures of commercial cryptography products.

3. Principle of Non-discrimination and Prohibition on Compulsory Technology Transfer

The rigorous regulation of the Regulation of Commercial Encryption Codes has led to limited acquisition of licenses by foreign invested enterprises. Because the Cryptography Law formally cancelled these licenses, foreign invested enterprises may be treated equally with Chinese enterprises in the future. Of course, certificates of commercial cryptography products models, importation licenses and annual filings of sales figures mentioned above should be acquired by foreign invested enterprises as applicable/required.

In response to foreign companies’ concern about compulsory technology transfer imposed by the Chinese government, the Cryptography Law, like the Foreign Investment Law, reiterates the principle of non-discrimination against foreign invested enterprises and prohibits compulsory transfer of commercial cryptography technology. In addition, under the Cryptography Law, cryptography administration and its staff are now obliged to keep confidential the commercial secrets and personal information discovered during the performance of their responsibility, and prohibited from asking cryptography enterprises and certification institutions to disclose cryptography-related proprietary information such as source code.

4. Connection with Cybersecurity Law

The Cryptography Law clarifies the connection between the use of commercial cryptography and some compliance requirements under the Cybersecurity Law:

- Commercial cryptography products involving national security, national economy and people's livelihood, and public interests should be included in the critical network equipment and the catalogue of specialized cybersecurity products, and those products shall not be sold before certification by qualified institutions.

- If some critical information infrastructure (CII) is required by law to be protected by commercial cryptography, its operator (CIIO) shall use commercial cryptography to protect the critical information infrastructure, and by itself or by engaging a qualified institution, conduct a security evaluation. Under the classified protection of information system security, CII should in principle be protected under level three and encrypted by cryptography. Therefore, in
principle, all CIIOs shall conduct the aforementioned security evaluation on the use of commercial cryptography. If a CIIO fails to use commercial cryptography or fails to conduct security evaluation on the use of commercial cryptography as required under the *Cryptography Law*, and such failure causes detriment to cybersecurity, the CIIO may be penalized for a fine ranging from RMB 100,000 to RMB 1 million, and a personal fine may be imposed on responsible persons ranging from RMB 10,000 to RMB 100,000.

- If the CIIO’s purchase of cyber products and services involves commercial cryptography, which may affect national security, the CIIO shall undergo national security review, in accordance with the *Cybersecurity Law*, as organized by the cyberspace authority together with the relevant departments such as the state cryptography administration. If a CIIO fails to conduct national security review as required under the *Cryptography Law* or uses products which fail to pass the national security review, the CIIO may be ordered to suspend the use of the cryptography products and penalized for a fine ranging from one to 10 times the purchase price of such products, and a personal fine may be imposed on responsible persons ranging from RMB 10,000 to 100,000.

**The Baseline for Cybersecurity Classified Protection is Formally Released**

On Dec. 1, 2019 the *Information Security Technology - Baseline for Cybersecurity Classified Protection (MLPS 2.0)* took effect. This national standard explicitly stipulates the *Cybersecurity Multi-Level Protection Scheme (MLPS)* in all respects, as well as the predecessor of the MLPS 2.0 is the *Computer Information System Security MLPS (MLPS 1.0)*, practiced in China for more than 20 years. The major differences between MLPS 1.0 and MLPS 2.0 are that: (i) MLPS 1.0 mainly applied to security of information systems based on traditional structures, while the scope of the protected subjects in MLPS 2.0 is expanded to cyberspace by including new technologies and application scenarios such as cloud computing, big data, and Internet of Things; (ii) protection under MLPS 1.0 focused more on the security protection of systems, staff and physical environment, while protection under MLPS 2.0 has been amended to emphasize security of cyberspace systems surrounding data, networks, systems, and staff. MLPS 2.0 is a hierarchical protection mechanism for information systems, and the more important the system is, the more stringent the protection requirements are. As the fundamental cybersecurity policy of China, MLPS 2.0 requires enterprises to find out the security risks of the information systems through MPLS assessment, make rectification in accordance with and continuously comply with the relevant requirements under MLPS 2.0, so as to improve the information security protection ability of their own information systems, which, on the other hand, may result in increased compliance costs related to cybersecurity for the enterprises.

Under MLPS 2.0 and other relevant laws and regulations (e.g., the *Cybersecurity Law*), enterprises shall fulfill the following basic MLPS-related obligations: (i) completing grading, assessment, and record filing; (ii) issuing internal security policies and procedures and designating persons in charge of network security; (iii) taking technical measures to prevent actions that may harm network security, such
as a computer virus, cyber-attack, and network intrusion; (iv) taking technical measures to monitor and record network operation status and network security incidents, and retain relevant network logs for at least six months; and (v) taking measures to categorize data and back up and encrypt important data.

The grading, assessment, and record-filing under the MLPS 2.0 requires the enterprises’ special attention with respect to the following: (i) The MLPS filing is not equal to the MLPS assessment. In some practical cases, although some enterprises have completed the MLPS filing with the public security authorities, they fail to go through the MLPS assessment, and are therefore subject to administrative penalties imposed by competent authorities (usually refers to an order for correction or a fine of RMB 10,000 to RMB 100,000). (ii) Even if a company engages an assessment agent to assess its network system for grading, the company is responsible for the accuracy of the grading of its network system. Also, if a company is graded level II or above, it shall file with the competent public security authority within 30 days of the confirmation of its grade.

The Promulgation of the New Rules Concerning Collection and Use of Personal Information by Mobile Internet Applications

On Dec. 30, 2019, the Ministry of Industry and Information Technology, the Office of the Cyber Security and Information Technology Commission, the Ministry of Public Security and the State Administration for Market Regulation jointly issued the Measures for Determining the Illegal Collection or Use of Personal Information by Apps (the Measures). The Measures describe the typical methods by which mobile internet applications (Apps) may collect and use personal information in violation of laws and regulations. In addition to providing clear supervision standards for the regulatory authorities, the Measures also assist App operators with compliance management.

According to the Measures, the following four types of behaviors constitute illegal collection and use of personal information:

- **Non-compliant collection method.** The following conduct may be deemed unlawful in relation to the collection of personal information: (i) where the App fails to provide the user with notice of the collection and use rules; (ii) where the App fails to expressly provide notice of the purpose, method or scope of collection and use of personal information by third party SDKs and APIs (including failure to notify the user in a proper manner once such purpose or scope changes); or (iii) where the App collects and uses personal information without the user’s consent, uses a pre-checked box confirming consent as a default option, or does not provide the user with the option to withdraw consent (e.g., collecting personal information before obtaining the user’s consent or after being refused by the user).

- **Non-compliant collection content.** An App shall not collect or use the personal information which is unrelated to the services it provides (e.g., the existing
business functions of the App). If an App refuses to provide business functions because the user refuses to consent to the collection of non-essential personal information, such conduct of the App will be deemed illegal.

- **Non-compliant sharing or transferring.** Apps are prohibited from directly providing personal information to any third party without the user’s prior consent or without anonymizing the personal information prior to sharing.

- **Non-compliant information management assurance.** Such violations committed by Apps mainly include: (i) failure to process user requests to correct or delete personal information and cancel accounts, or setting unnecessary or unreasonable pre-conditions; and (ii) failure to respond to users’ corresponding request of operation in a timely manner (within 15 business days as the response time limit).

©2020 Greenberg Traurig, LLP. All rights reserved.

**Source URL:** [https://www.natlawreview.com/article/china-newsletter-spring-2020-direct-investment-compliance](https://www.natlawreview.com/article/china-newsletter-spring-2020-direct-investment-compliance)