31 August 2015

Who will be affected by the new regulation of banking security?

It is reported that the China Banking Regulatory Commission ("**CBRC**") is going to reintroduce new banking safety rules (the "**Revised Regulation**") and has consulted representatives of western technology enterprises such as Microsoft, IBM and Cisco about the Revised Regulation. It appears that the Guidelines to Promoting the Application of Safe and Controllable Information Technologies to the Banking Industry (2014-2015) (the "**No.39 Guideline**") and the Guiding Opinions of the CBRC on Strengthening Banking Network Security and Information Technology Construction through the Application of Safe and Controllable Information Technologies (the "**No.317 Guiding Opinion**")that were suspended on April 2015 will be implemented again having been revised to better promote and protect the information and technology security of the financial industry in China.

In recent years, the Chinese government has introduced a series of laws and regulations to strengthen the protection of information and technology security. Apart from the No.39 Guideline and the No.317 Guiding Opinion, both the State Security Law of the People's Republic of China (effective on 1 July 1 2015) (the "**State Security Law**") and the Cyber Security Law of the People's Republic of China (Draft) (promulgated on 15 June 15 2015) (the "**Cyber Security Law (Draft)**") reflect the great importance China attaches to information security.

Since the Revised Regulation has not been accessible to the public, this article will address the influence, on financial institutions and their equipment and technology suppliers, of the No.39 Guideline, No.317 Guiding Opinion, State Security Law, Cyber Security Law (Draft) and WTO Agreement on Subsidies and Countervailing Measures ("**SCM Measures**")

The scope of the Revised Regulation

The No. 317 Guiding Opinion applies to all financial banking institutions incorporated in the PRC, but whether it also applies to foreign banks (especially their branches in China) is still controversial. The draft Cyber Security Law aims to protect the important information systems of the financial industry. The subsidiaries and branches of overseas financial institutions inside the PRC are all within the category of key information infrastructure operators, which are subject to the draft Cyber Security Law and other relevant regulations.

Although the CBRC is not clear on this point, we consider that the No. 317 Guiding Opinion does apply to foreign bank branches in PRC and the Revised Regulation may clarify this.

The requirement for safe and controllable information technology

The No.317 Guiding Opinion defines “safe and controllable information technology” as “information technology which can meet bank demands for information safety, and which controls technical, outsourcing and supply chain risks”. The No.317 Guiding Opinion also divides information technology products and service (including all kinds of equipment, software and technical services) into 10 categories with more than 60 subclasses. Each class of products or services must comply with a corresponding safety and control requirement. In other words, all of a bank’s IT products and services must meet the same safety and controllability standard under the No.317 Guiding Opinion.

However, it is this strict safety and control requirement that is causing concern among majority foreign-owned enterprises (especially IT enterprises). They have four main issues. First, the suppliers of most technical products and services must have a technology research and development and service center in the PRC. Second, a Chinese citizen, business entity or unincorporated body must have an unfettered right to use or some right of control over the use of certain IT products. Third, the source code for some IT products must be filed with the IT department of the CBRC for the record. Fourth, the supply chain risks of most IT products must be dealt with, which implies that the suppliers of technology must be highly localized.

In relation to these four requirements, both the CBRC and banking firms have focused their attention on whether the suppliers have independent ownership and control over the IP rights to use the relevant technology and products. Although the No.317 Guiding Opinion provides that the software to be secured and controlled must have an unfettered use of the IP rights, it only requires the software suppliers to provide certification of their IP rights or their legitimacy without considering territorial rights and it lacks a clear definition of the needed extent of the financial institutions independent ability to use the IP rights. Therefore, we think that the standard for determining whether a financial institution has an independent ability to use the IP rights will be one of the highlights of the Revised Regulation.

In addition it is worth mentioning the further expansion of the requirements to provide for safety and controllability. The CBRC intends to supervise foreign-owned enterprises which want to joint venture, or to set up an R&D center and share IP rights in China so as to manage safety and controllability. In the process of promoting the localization of technology, China is likely to not only consider the foreign enterprises’ experience and technology in financial services, but will also set strict safety and controllability requirements. By virtue of article 29 of the draft Cyber Security Law, if operators of key information infrastructure want to buy network products or services, they must enter into a confidentiality agreement with suppliers. Article 59 of the State Security Law also incorporates network products and services within the scope of national security review and supervision. Hence in the future, for suppliers of network products or services to financial institutions in PRC, the market access threshold will be

higher and safety requirements will be stricter.

The application of safe and controllable information technology

The No.39 Guideline requires from 2015, an annual increase of no less than 15% in the use of safe and controllable information technologies in all banking financial institutions to a total of no less than 75% by 2019. The general framework of No.317 Guideline set the proportion of the category of safe and controllable information technology required to be achieved in 2014-2015. This mandatory proportion illustrates the Chinese government's determination to promote cyber security and to some extent provides support to the local financial services industry. Chinese enterprises will be the biggest beneficiary and an obvious challenge to financial service enterprises in foreign countries, including USA, Europe and Japan. Foreign enterprises believe the Revised Regulation will shut them out of a financial service market which has an estimated value of US$500 billion.

We think that the overall position on safe and controllable technologies set out in the No.39 Guideline will remain unchanged. Mastery will be obtained over the core knowledge and key technologies for banking information systems aiming to achieve a secure and controllable information technology usage rate of 75% plus by the end of 2019. However the key point of the Revised Regulation will be the setting of the proportion of safe and controllable technologies to be applied. Considering the gap between Chinese and foreign core equipment and technology, the trade flow between China and western countries and the tolerance of local large enterprises to the opening of their IT market, the Chinese government will tend towards a stable development strategy. It will wish to harmonize and balance the relationship of all the parties. Therefore in order to ensure its feasibility and wide acceptability, the Revised Regulation will address all of: the annual proportion to be achieved, the detailed requirements for implementation, and the scope of application, of safe and controllable technology.

Information technology budgeting by banking financial institutions

The No.39 Guideline requires bank financial institutions to spend no less than 5% of their annual information technology budgets from 2015 exclusively on research and development of safe and controllable information systems and to master core information knowledge skills. Since the national commercial banks in China are recognized as "public institutions" under the SCM Measures by the WTO panel and appeal body, this 5% expenditure may violate WTO regulations on subsidies. Spending by government owned entities to develop technology is likely to be recognized as a subsidy under WTO regulations.

It is our view that national and financial security is politically sensitive since it has a direct impact on national sovereignty. Moreover, because of the importance of network and IT security its protection will become a more regular and normal practice in China and the necessary measures to ensure cyber security will be undertaken validly within the WTO framework.

Conclusion

Given China's weak development of science and technology in the financial sector as well as the current national condition, the Revised Regulation is likely to be relatively inclusive and less restrictive of foreign invested enterprises. However, there will be no change to the determination and efforts of the Chinese government to promote cyber security and locally owned intellectual property rights. In any event, influenced by the proactive compliance culture of the banking industry, it is possible that some banks will already comply with the standards in the No. 317 Guiding Opinion. Foreign financial equipment and information enterprises in PRC should take note of the passage of the Revised Regulation and prepare for these fundamental changes by sharing intellectual property and setting up R&D and service centres so as to embrace the challenges brought by the new regulation of information technology in the banking sector.

Editor's note: This article was simultaneously published on Chinalawinsight.com

This article was originally written in Chinese, and the English version is a translation.

Categories: China Bulletin | Banking & Finance

Key contact

Armstrong Chen
Partner
Beijing, Shanghai
T +86 10 5878 5588