Linklaters

9 September 2015

National Security Considerations in China's Financial Sectors – an International Perspective.

National Security Considerations in China's Financial Sectors – an International Perspective

Background

China's National Security Law[1] and its subordinate laws and regulations, some of which are still drafts,[2] raise a wide range of issues under the label of "national security" for policy makers, investors and other stakeholders. By consolidating existing regulations and introducing new requirements, giving them the status of national law, the new law paves the way for existing legal concepts to be more broadly defined in future regulations. For financial institutions, the new law may lead to increased regulation in financial transactions, IT architecture, data protection and other aspects of daily operation.

Though the National Security Law's function is to set out broad principles without a corresponding sanctions regime, the implications for its future implementing rules are profound. Accordingly, this guide introduces the key considerations which the new national security regime poses for financial institutions operating in the PRC,[3] including their business relationships with entities in the PRC.

PART A: GENERAL REQUIREMENTS

Security of the financial system

The PRC government's concerns of preventing systemic and regional financial risks and defending against the impact of external financial risks are included in the National Security Law as part of the elements that go towards

[1] National Security Law of the PRC (中华人民共和国国家安全法), 1 July 2015.

[2] These primarily include: Anti-Terrorism Law of the People's Republic of China (Draft) （中华人民共和国反恐怖主义法（草案））, 3 November 2014; Cyber Security Law of the PRC (Draft) （中华人民共和国网络安全法（草案））, 6 July 2015; and Trial Measures on National Security Review of Foreign Investment in Free Trade Zones （自由贸易实验区外商投资国家安审查试行办法）, 8 May 2015.

[3] As used in this note, "PRC" refers to mainland China (not including Hong Kong, Macao and Taiwan).

Contents

the maintenance of national security, sitting alongside such objectives as food security, strategic resources and cultural sovereignty.

To achieve financial stability within the broader context of the continuing liberalisation of China's financial markets and the RMB, the PRC government is expected to replace the current system of approvals and other direct controls with a more indirect approach that still preserves regulatory flexibility (for example, macro-prudential financial management tools which allow for the tightening or loosening of policy according to economic conditions). This is being tested in certain free trade zones in the PRC, where a macro-prudential parameter is embedded in the calculation of foreign debt limits, adjustable in accordance with capital movements and credit conditions or to the extent the scale of offshore financing needs to be limited on a temporary basis in the interests of national financial stability.[4]

Although such measures may to a certain extent cast doubt over the pace of liberalisation of China's financial markets in the face of greater macroeconomic instability, reform of the financial markets is expected to continue in a way which will benefit China in the long term – such as the change from an approval-based to a registration-based IPO system.

National security review

A national security review was introduced in the PRC in 2011 to enable more systematic monitoring of foreign investments in sensitive sectors, with an associated sanctions regime requiring the disposal by foreign investors of investments not submitted for review as required, and which were subsequently determined to have (or to be likely to have) a material impact on national security.

Today, specific rules concerning national security review in the financial sector, though contemplated by the regime, have yet to be released. However, the expansion of the 2011 regime has taken shape through new rules issued in the free trade zones in May 2015 (see our earlier alert) which themselves embody the key principles of the national security review regime in the Draft Foreign Investment Law (which aims to achieve fundamental change in China's foreign investment regime) published by the Ministry of Commerce in January 2015. The free trade zones operate as a testing ground for new laws and regulations before they are introduced at national level.

We would, accordingly, expect many key principles of the expanded regime to be applied to the financial sector as well. Below are some issues that may pose particular concerns in the financial sector:

Regime extended to greenfield investment: the 2015 revisions extend foreign investments subject to national security review to greenfield investments (which is how many foreign financial sector investments are

[4] Experimental Implementing Rules for Macro-prudential Management of Overseas Financing of Separately Accounted and Audited Business Units and Cross-border Fund Flows in the China (Shanghai) Free Trade Zone （中国（上海）自由贸易试验区分账核算业务境外融资与跨境资金流动宏观审慎管理实施细则（试行））, 12 February 2015.

structured), while the scope of transactions covered by the existing national rules, which apply throughout the PRC other than in the free trade zones, only includes acquisitions of existing assets and businesses.

Investment review factors: the National Security Law adopts a wide definition of "national security" which covers popular welfare, sustainable economic development and other vital interests of the State. Both the Draft Foreign Investment Law and the rules of the free trade zones prescribe an extensive list of factors to be considered in the national security review process, including the impact on key infrastructure and technology and whether the investments are made by persons controlled by a foreign government. These all signal that the factors guiding national security review of foreign investment in the financial sector, when the regime is finally put in place, are likely to be broad.

Key technology: the National Security Law expands the national security regime beyond foreign investment review, to include key technologies and network information technology products and services which may affect national security. This expansion may pose particular concerns to international financial institutions operating in the PRC, given the cross-border nature of their organisational structures and the characteristics of their operations.

Prevention of terrorism

The prevention of terrorism is a key aspect in maintaining both national security and the security of the financial system. The Draft Anti-Terrorism Law reiterates the existing rules requiring financial institutions to conduct client identification and report suspicious transactions in order to prevent terrorism.

In addition, the draft law goes further, in requiring that an institution (including a financial institution) must not facilitate, assist or transact with terrorist institutions or individuals and must report all such findings to the public security authorities.

The next step may be for more detailed rules to be issued, which may ultimately impose more extensive obligations on financial institutions to conduct due diligence on certain clients and transactions and to cooperate with public security/national security authorities. In turn, the tightening of regulation in this area poses new challenges for financial institutions seeking to enter the mobile/internet payments market (characterised by large volumes of small transactions, for which extensive diligence requirements are impractical).

PART B: IT INFRASTRUCTURE

Article 25 of the National Security Law stipulates that the Chinese State shall develop systems to ensure the security of its networks and information, achieve secure and controllable information systems and data in key areas, prevent, deter and punish IT crime (such as disseminating harmful information over the internet), and safeguard the IT sovereignty of the State.

As further illustrated in the Draft Cyber Security Law, which aims to legislate holistically for the protection of the sovereignty and integrity of China's IT networks, construction of a secure and stable network to withstand outside influence and interference is a main part of the national security strategy. Particular emphasis is placed on maintaining the integrity of "key information infrastructure", which spans a wide range of regulated sectors of China's economy including telecoms, broadcasting, energy, transport, water conservancy and finance.

General requirement to develop "secure and controllable" infrastructure

Under the National Security Law, the strategic positioning and directional guidance of how key network infrastructure is to be sourced and developed is a key objective. Article 24 provides for the development of "independent and controllable … core critical technologies in key areas", while Article 25 contemplates "the security and controllability of network and information core technologies". As shown in the CBRC and MIIT's Joint Guidance,[5] which called for the development of "independent core applications, core knowhow and key technology" even before the National Security Law was passed (and which has been extensively covered in our earlier alert), the banking sector is likely to be one of the key sectors in which the principles of Articles 24 and 25 will be applied.

Within the context of the new law and its wider regime, reasonable interpretation would suggest that the consistent use of the word "controllability", although undefined, contemplates not only the key technology owner/infrastructure operator's ability to control technical risk, but also the government's ability to direct the use of and access to networks without the co-operation of external parties (for example, the Joint Guidance combines national security requirements with those for innovation, independence, security and controllability).

As many of the proposals are still in draft form and the revision of rules which will put the Joint Guidance into effect (currently in the form of the suspended Bank IT Guidance)[6] is still awaited, it is not entirely clear how these requirements will be implemented for banks. The proposals and principles released so far do, however, give a broad indication of the Chinese government's security priorities and financial institutions should plan for their future IT requirements with them in mind.

---

[5] Guidance Opinion of the China Banking Regulatory Commission ("CBRC"), National Development and Reform Commission, Ministry of Science and Technology, and Ministry of Information Industry ("MIIT") on the Use of Secure and Controllable Information Technology to Strengthen Network Security and Informatisation of the Banking Industry (关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见), 3 September 2014 (the "Joint Guidance").

[6] Notice of the General Offices of the CBRC and the MIIT on the 2014-15 Guidelines for Secure and Controllable Information Technology in the Banking Industry (中国银监会办公厅、工业和信息化部办公厅关于印发银行业应用安全可控信息技术推进指南（2014 - 2015 年度）的通知), 26 December 2014 (the "Bank IT Guidance").

Supplier/partner selection

The impending introduction of security and controllability requirements as discussed above may ultimately result in domestic IT equipment and solutions being preferred over foreign ones, in order to meet the additional compliance requirements. For example, the Joint Guidance contains key directives for banks to:

- increase their proportion of "secure and controllable" IT;
- give priority to technology and solutions which are more open, transparent and broadly applicable;
- co-operate with institutions which are willing to co-operate in respect of core knowledge and key technologies; and
- avoid reliance on a single product or technology.

Though implementing rules which originally provided a timetable for how these goals are to be achieved (in the form of the Bank IT Guidance) have been informally suspended by the CBRC, global IT solution providers are already seeking the development of local solutions through partnerships with domestic entities, in anticipation of more specific "independence" and "controllability" requirements being issued. It is worth noting that the Bank IT Guidance had set out specific criteria for each category of IT product and service of banks, in most cases including suppliers having R&D and service centres in China and the associated software containing indigenous Chinese intellectual property.

Further, the Draft Cyber Security Law proposes a national security review process for key information infrastructure operators (including financial institutions) purchasing network products and services that may influence national security, with the implementation rules still to be issued by the State Council. Though the content of the review is still unknown, the Bank IT Guidance already suggests an overall desire to impose regulatory review requirements on core systems (such as requirements to register source code powering operating systems, database software and middleware with the CBRC).

Financial institutions therefore need to consider the potential impact of the proposed changes in evaluating potential suppliers to build out or upgrade their existing networks. It will also be interesting to see how the "independence" and "controllability" requirements can apply to foreign equipment for which no alternative is available domestically, and whether the authorities will extend any flexibility in this regard. In such cases, the use of foreign equipment and solutions could still involve a more protracted process as a result of the changes.

IT specifications/certifications

More specifically, Article 19 of the Draft Cyber Security Law would permit network operators and their third-party outsourcers to use only those products that have passed certification or security testing as equipment for key

networks or for cyber security purposes. The Draft Cyber Security Law would require the national cyberspace administration authority, together with other ministries, to develop a catalogue of key network equipment and products specifically for IT security purposes and implement mutual recognition of security certification and inspection testing. The details are, however, unclear and it is uncertain whether it will lead to additional burdens (such as bringing new categories of equipment/solution within the scope of the rules, or introducing new certification/testing requirements) when implemented, despite the stated intention of the draft law to eliminate duplication of effort.

Pre-installed "backdoors" and pre-clearance of encryption schemes

In addition to these review requirements, what is more worrying is that the Draft Anti-Terrorism Law proposes to require certain features to be embodied in all networks, including preinstalled technical interfaces which can be used as security "backdoors" by the government authorities in preventing or investigating terrorist activities, and encryption schemes to be submitted to relevant PRC authorities for approval. In combating terrorism, the Draft Anti-Terrorism Law would empower the public security and state security organs to use telecommunications and internet technical interfaces to prevent and investigate terrorism, including requiring service providers/users to provide technical support for decryption.

IT network regulation

Levels of protection: the State Council is empowered under the Draft Cyber Security Law to formulate a classified IT security protection system, as well as specific rules on the safety of financial institutions' important IT. The concern here is whether, and to what extent, the State Council's rules will go further than the existing IT security regulatory regime, thus imposing more compliance burdens.

Key protective measures: the Draft Cyber Security Law would compulsorily require services such as network access and information publication to be provided on a real-name basis.

In addition to routine compliance, more extensive obligations that would be imposed by the Draft Cyber Security Law include the categorisation of network data for the purpose of back-up and important data encryption, and putting in place an IT security emergency response plan and periodic drills. The Draft Cyber Security Law would also require operators of key information infrastructure to conduct, or appoint a specialist firm to conduct, tests and evaluations on their networks' security and possible risks and report the results and corrective action to the responsible State Council departments for safety (including the relevant industry regulator and other departments) on at least an annual basis. These may significantly increase the costs to the network operators, including financial institutions, particularly given that the Draft Cyber Security Law and Anti-Terrorism Law overlap in some areas where the relationship between the two separate regimes is unclear.

PART C: DATA SECURITY AND ONSHORING

Banks are currently required to store, process and analyse all their personal financial information in the PRC, and are prohibited from transferring personal financial information out of the PRC in the absence of specific rules and regulations.[7] However, thus far it has been the accepted practice among foreign banks in the PRC for cross-border data transfer arrangements to be implemented with customer consent. The draft laws seek to expand these restrictions on transferring data out of the PRC beyond the banking sector and, if implemented, will affect how both onshore and offshore financial institutions structure their operations.

Data onshoring

Both the Draft Cyber Security Law and the Draft Anti-Terrorism Law propose data onshoring requirements with slightly different emphases. Read together, potentially, all corporate and personal data of domestic users obtained by any onshore internet service provider (including key information infrastructure operators such as banks and other financial institutions) through the provision of services in the PRC must be stored onshore in the PRC, and not transferred offshore (noting that the proposed requirements do not limit these prohibited transfers of data to internet transmission and could extend to physical and other forms of transmission), unless (i) otherwise permitted under law or regulation or (ii) a security assessment by the IT security and other State Council departments is completed (details of the process are not yet available).

The effect of the above requirements could be profound, including in the following areas:

- **Onshore infrastructure buildout:** international financial institutions' business models that are based on intra-group shared facilities could be significantly affected, with separate IT facilities having to be located onshore. Offshore legal and operational support (such as KYC and other data processing), client referrals by onshore to offshore units as well as internal auditing of onshore units by offshore headquarters may be made more difficult by the prohibitions against cross-border data sharing.
- **Diligence:** offshore service providers (such as financial advisers to PRC clients) will need to satisfy themselves that the cross-border transmission of information by PRC clients to them complies with the rules and does not need to go through national security assessment or, alternatively, that all relevant requirements have been met.
- **Reduced information flow:** in light of the proposed changes, offshore service providers may also consider restricting information flow from PRC clients (in particular, information that is identifiable to

[7] Notice of the People's Bank of China ("PBOC") on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Data (中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知), 1 May 2011.

the specific underlying clients of their PRC clients) to the extent feasible.

Protection of personal data

The Draft Cyber Security Law reiterates the current rules, which require financial institutions to prevent leakage, damage and loss of personal data and immediately rectify and report all such incidents to the competent authorities. Data subjects can require the financial institution to correct errors in the data it holds, and their consent must be obtained for their relevant information to be collected.

More broadly, the Draft Cyber Security Law refers to different degrees of obligation being imposed in further detailed rules to classify data and back up/encrypt important data, depending on the perceived risk for the relevant data network. There is as yet no draft of these segmented rules available. Given the national legal status of the general obligations and their wide scope, it is possible that these rules, when passed, would result in additional personal data protection requirements.

Data monitoring

The National Security Law requires public participation in national security efforts through ongoing monitoring and reporting, and places all citizens, enterprises and organisations of the PRC under a duty to protect national security.

The Draft Cyber Security Law and Draft Anti-Terrorism Law follow suit with proposed additional monitoring obligations that require network operators to be gatekeepers of the information published through their networks and monitor the information that is being disseminated to their users over their networks. If any dissemination of illegal information (such as information inciting ethnic discrimination, disturbing social order or relating to pornography, gambling, violence, murder or terrorism) is detected, the operator must immediately cease the transmission of the data, keep records of the transmission and report to the IT security authorities. As network operators, financial institutions would also be bound to comply with these obligations in relation to external and internal dissemination of information over their networks.

Key References

National Security Law of the PRC (中华人民共和国国家安全法), 1 July 2015 (the "National Security Law").

Anti-Terrorism Law of the People's Republic of China (Draft) (中华人民共和国反恐怖主义法（草案）), 3 November 2014 (the "Draft Anti-Terrorism Law").

Cyber Security Law of the PRC (Draft) (中华人民共和国网络安全法（草案）), 6 July 2015 (the "Draft Cyber Security Law").

Guidance Opinion of the China Banking Regulatory Commission ("CBRC"), National Development and Reform Commission, Ministry of Science and Technology, and Ministry of Information Industry ("MIIT") on the Use of Secure and Controllable Information Technology to Strengthen Network Security and Informatisation of the Banking Industry (关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见), 3 September 2014 (the "Joint Guidance").

Notice of the General Offices of the CBRC and the MIIT on the 2014-15 Guidelines for Secure and Controllable Information Technology in the Banking Industry (中国银监会办公厅、工业和信息化部办公厅关于印发银行业应用安全可控信息技术推进指南（2014 - 2015 年度）的通知), 26 December 2014 (the "Bank IT Guidance").

Notice of the People's Bank of China ("PBOC") on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Data (中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知), 1 May 2011.

Authors: Grace Yu; Bryan Chan

Contacts

For further information please contact:

Jian Fang
Partner

(+86) 21 2891 1858

jian.fang@linklaters.com

Betty Yap
Partner

(+852) 2842 4896

betty.yap@linklaters.com

Richard Gu
Senior Consultant

(+86) 21 2891 1839

richard.gu@linklaters.com

Grace Yu
Managing Associate

(+86) 21 2891 1819

grace.yu@linklaters.com

Adrian Fisher
Managing Associate

(+65) 6692 5856

adrian.fisher@linklaters.com

Linklaters LLP Shanghai Office
29th Floor, Mirae Asset Tower
166 Lujiazui Ring Road
Shanghai 200120, China

Telephone (+86) 21 2891 1888
Facsimile (+86) 21 2891 1818

Linklaters
10th Floor, Alexandra House
Chater Road, Hong Kong

Telephone：(+852) 2842 4888
Facsimile： (+852) 2810 8133

Linklaters Singapore Pte. Ltd.
One George Street #17-01
Singapore 049145

Telephone (+65) 6692 5700
Facsimile (+65) 6692 5708

A30299644/0.17/09 Sep 2015