Client Alert

March 16, 2015

International IT Companies Face Continuing Headwinds in China

By Paul D. McKenzie and Gordon A. Milner

Our September 16, 2014 client alert, "Brave New World? Recent Challenges Facing Foreign IT Companies in China," discussed efforts by the Chinese government to enforce heightened network security standards, with a particular focus on the issuance on September 1, 2014 by the Ministry of Industry and Information Technology ("**MIIT**") of the *Guiding Opinions on Strengthening Network Security in the Telecommunications and Internet Sectors* (关于加强电信和互联网行业网络安全工作的指导意见; the "**MIIT Opinions**").

A great deal has happened in the six months since the MIIT Opinions were issued. Developments include:

- the announcement of network security standards in the banking sector that have raised substantial concerns for both financial institutions and IT providers, including a growing concern among foreign IT companies ("**FITCs**") that the Chinese government's campaign to enhance network security is a thinly disguised "buy local" campaign; and
- the circulation of a draft Anti-Terrorism Law that contemplates Chinese government agencies being given very far-reaching powers to access data transmitted over the Internet and other telecommunications networks.

This client alert outlines these key developments and discusses their potential impact on FITCs.

BANKING STANDARDS – EVIDENCE OF A GROWING "BUY LOCAL" CAMPAIGN?

The banking sector appears to be at the vanguard of the Chinese government's network security campaign. Network security standards announced to govern the banking sector have potential significance far beyond that sector, since it seems likely that the experience implementing these new standards will inform the regulatory approach in introducing network security standards in other sectors in the future.

These banking standards reflect a clear distrust of the security of foreign IT products and services. They almost certainly also represent an effort by the Chinese authorities to help local products and services move up the IT value chain and reduce dependence on foreign IT. FITCs are reasonably concerned that their market access in China will be adversely affected.

On September 3, 2014, the China Banking Regulatory Commission ("**CBRC**"), the National Development and Reform Commission, the Ministry of Science and Technology, and MIIT issued the *Guiding Opinions Regarding Application of Secure and Controllable Information Technologies to Strengthen Network Security and Informization of the Banking Sector* (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; the "**Banking Opinions**").

The Banking Opinions encourage the use of "*secure and controllable*" (安全可控性) information technologies – adopting the same term that appears prominently in the MIIT Opinions and other government documents – and call for implementation of network security review standards for the banking sector. Other key provisions include the following:

- Specific goals for utilization of secure and controllable technologies in the banking sector are set: 15 percent in 2015 and no less than 75 percent in 2019.
- The importance of developing local technology is emphasized.
- Priority is given to technologies and solutions that are "highly open, highly transparent and of a broad application scope" and to suppliers who are willing to work on a cooperative basis in relation to key knowledge and critical technologies.

The Banking Opinions were followed by issuance by the CBRC and MIIT on December 29, 2014 of the following:

- the *Implementing Guideline for Promoting the Application of Secure and Controllable Information Technology in the Banking Sector* (2014–2015) (银行业应用安全可控信息技术推进指南(2014–2015年度; the "**Guideline**"), which is appended with
- the *Classification Catalogue of Banking Information Technology Assets and Security and Controllability Targets for the Banking Sector* (银行业信息技术资产分类目录和安全可控指标; the "**Catalogue**").

The Guideline and Catalogue implement the Banking Opinions by defining specifically what "security and controllability" require in regard to stipulated categories of IT products and services. The Catalogue covers a very wide range of products and services in considerable detail – specifically addressing some 50 sub-categories of hardware (ranging from mainframes, through specialized banking hardware like ATMs to fungible items like printers), 12 sub-categories of software (including operating systems and office software in addition to specialized banking applications), and 6 types of technical services (including consulting, development, and outsourced operations). For each sub-category, the Catalogue sets out "security and controllability" criteria together with minimum utilization rates to be achieved in 2015.

The Guideline specifies that it applies to all banking financial institutions established within the PRC. We understand that the term includes commercial banks as well as policy banks, financial asset management companies, and other financial institutions under the direct supervision of the CBRC and does not include, for example, international trust and investment companies, which are not under CBRC supervision. For the balance of this Alert, we use the generic term "bank" to refer to banking financial institutions governed by the Guideline.

It is beyond the scope of this Alert to discuss in detail the specific criteria for being secure and controllable for each category of IT product and service. However, criteria that are causing FITCs concern about their continuing access to the Chinese market include the following:

- For all of the various categories of software product and (in respect of firmware and embedded software components) many of the categories of hardware products listed in the Catalogue, source code is required to be submitted to the CBRC. Many vendors consider the source code to their products to be highly sensitive for both intellectual property protection and security reasons and have historically declined to file source code with public authorities even at the cost of missing out on the enhanced

protection afforded under the existing voluntary Chinese copyright registration regime for source code. As such, the requirement for mandatory submission of source code has caused particular concern among FITC vendors. It appears that those concerns are at least partially recognized by the CBRC. In a notice on February 12, 2015, the CBRC commented that the details of the requirement to submit source code are still being investigated and will be implemented only after "various opinions have been heard."

- The embedded software (and, in some cases, hardware chips) used in almost all sub-categories of networking, storage, and security hardware is required to be "under indigenous IPR." Notes to the Catalogue explain this requirement as meaning that the intellectual property in those components must be either exclusively owned and controlled by a Chinese party or used by a Chinese party under long-term rights without restrictions on innovation. Further clarification will be required from the CBRC, but on its face, this requirement could force FITC vendors to produce separate "China-only" versions of their product lines and could make it extremely difficult for foreign banks to maintain globally standardized networks.

- Trusted computing modules utilized in various types of computer equipment must be those that have obtained certification as commercial encryption products in China – meaning in effect that they may not utilize the international TPM standard, which is not currently certified in China, and must use the Chinese TCM standard.

- All categories of IT hardware and software listed in the Catalogue are subject to the vague requirement that "technology risk and supply chain risk are controllable." Some commentators have suggested that this may be construed as requiring that relevant products be manufactured in China. This may be an overly conservative interpretation – though it is worth noting that many FITC products are, as a matter of fact, already manufactured in China.

- Suppliers of almost every category of IT hardware and software listed in the Catalogue are required to operate R&D and service centers within China, "providing continuous upgrades and technical support services" for products. While many major FITCs already possess facilities in China, those who do not will need to decide whether to establish local affiliates. From the point of view of the banks, this has the potential to cause problems for the use of foreign-developed open-source products – a point which will need to be clarified by the CBRC.

- A number of categories of IT product are subject to testing and certification requirements, without explaining the nature of the testing or identifying the certifying organization.

The benchmarks for minimum utilization vary significantly with the category of product or service. Perhaps reflecting the difficulties in replacing specialized software, the lowest rates (5, 10, or 15 percent, depending on the category of bank) apply only to procurement of "dedicated" banking software. A 100 percent rate applies to most categories of computer hardware and to all categories of security equipment, which may reflect the more fungible nature of such equipment.

The Guideline specifies in considerable detail the work that banks are expected to undertake to implement the requirements of the Guideline and Catalogue and the work of both CBRC and MIIT to support and evaluate banks in their implementation. It also sets out a March 15 deadline for each bank to submit a report to CBRC addressing matters such as the management organization it has put in place to oversee implementation of the

Guideline and Catalogue. The Guideline also encourages banks and IT companies to bring to the CBRC's attention difficulties and questions they encounter in regard to testing and certification and other requirements and provides that CBRC and MIIT will be equipped to start receiving from IT companies relevant filings and risk evaluation requests contemplated under the Catalogue beginning April 1, 2015.

DRAFT ANTI-TERRORISM LAW

On November 3, 2014, the National People's Congress ("**NPC**") issued the Anti-Terrorism Law (First Review Draft) (反恐法草案(一审稿)) for public comments.

The first draft of the law caused significant concerns among FITCs due to the following requirements:

- In their design, construction, and operation of telecoms and internet networks, telecommunications network operators and internet service providers must "preset" a technical interface and submit the encryption scheme with the authority responsible for encryption – vague language that commentators understand to mean that PRC government authorities would have broad rights to monitor network use.
- Telecommunication services providers and internet service providers must keep relevant equipment and data in respect of local users within the territory of China.

According to March 9, 2015 comments made by a representative of the legislative drafting committee of the NPC Standing Committee, a review of a second draft of the law was completed in February and, while the law is not on the agenda for the NPC session that convened on March 5, 2015, the law may undergo third reading and promulgation later in 2015.

In responding to questions about the draft law, spokesperson for the NPC, Fu Ying, is quoted by Xinhua news agency as stating that the second draft of the law stipulates that use of the technical interface (1) is limited for purposes of investigating and preventing terrorist activity, (2) is limited to public and state security agencies, and (3) is subject to a strict review and approval process.

OTHER DEVELOPMENTS IN REGARD TO NETWORK SECURITY

Network Security Convention

We have learned from an industry source that, on December 2, 2014, the National Information Security Technology Standardization Technical Committee of the China Communication Standards Association (中国通信标准化协会网络与信息安全委员会; "**NIST**") and China Information Security Certification Center (中国信息安全认证中心；"**ISCCC**") jointly distributed a Self-Discipline Convention on Safeguarding User's Network Security by Information Technology Product Suppliers (信息技术产品供应方维护用户网络安全自律公约; "**Convention**") to a limited circle of IT companies, who were invited to be founding signatories to the Convention.

The initial draft of the Convention covers a wide range of IT products and services, including hardware, software, systems, and services having capabilities that include storage, processing, transmission, control, exchange and display of information or data, including computers and peripherals, communications equipment, network equipment, automatic control equipment, operating systems, databases, application software, and services.

It includes covenants relating to collection, storage, and use of both personal data and information related to the State.

One key focus of the draft Convention is the control of remote control interfaces (sometimes known as "backdoors") in IT products. Specific covenants in regard to network security include the following:

- Remote control of user products is allowed only to the extent required for product maintenance or other purposes. Users must be expressly informed of the purpose of remote control and the ports and protocols used. Users should have the ability to disable remote control and be informed of the loss of function if they do so. Express consent of users is required for remote control, and users must be provided with real-time information about the status of remote control.
- Products should not include a covert interface or any module without an express function and components should not be installed that can disable or bypass security mechanisms. Any interface for testing or maintenance should be disclosed to users and should be capable of being shut down by users.
- Users should have the ability to schedule remote control, and records of data input and output during the remote control process should be maintained.
- In necessary cases, IT product suppliers should provide a relevant government-accredited third-party institution with the method and evidence that can be used to test and verify activity, such as collection of user information and remote control of user products.

Recent inquiries with officials at ISCCC suggest that the Convention has not yet been signed and may be subject to revision.

Health Care Measures

In May 2014, the National Health and Family Planning Commission issued the *Administrative Measures on Management of Population Health Information* (人口健康信息管理办法(试行); the "**Measures**").

The Measures contemplate relatively detailed restrictions on the collection, storage, and utilization of personal health information by various categories of health care providers, including a prohibition on the use of servers outside China for the storage of such information.

Interestingly, the Measures provide that all IT products on China's health care IT systems must obey the "national network security review regime," without specifying what that review involves, providing further evidence, if evidence is needed, that the Chinese government continues to work toward a network security review regime that reaches beyond merely the banking sector.

LOOKING FORWARD

The Chinese government has signaled clearly and repeatedly its commitment to increase network security, and so FITCs cannot expect related market access problems to abate – quite the opposite.

The coming weeks will see banks in China scrambling to understand the requirements of the Guideline and Catalogue, FITCs and domestic IT suppliers seeking to qualify their product offerings, and intense lobbying by banking institutions and IT suppliers, as well as by the United States, the European Union, and other foreign governments for an easing of the requirements.

Foreign banks operating in China will already have had to submit initial reports to their local CBRC offices in respect of the implementation of the Guideline and Catalogue. The new rules will cause a major headache for banks that have spent recent years seeking to optimize efficiency and security by standardizing IT hardware, softwares and networks across their global organizations. The integration of novel, locally developed Chinese systems into a bank's global IT systems may itself trigger further regulatory testing and approval requirements from the bank's overseas regulators. Moreover, the difficulties of implementing potentially major and intricate changes to banks' China IT systems may be exacerbated if the FITC consultants and system integration providers that helped build the banks' existing systems gradually elect to cede the market to local providers.

Meanwhile, Chinese regulators will likely turn their sights to network security beyond the banking sector. In its *Twelfth Five-year Plan for Information Security Industries (2011 to 2015)* (信息安全产业"十二五"发展规划), MIIT identified e-government, e-commerce, e-healthcare, finance, energy, transportation and distance education as sectors where use of secure and controllable IT products and services should be enhanced. Some of these sectors may soon be the target of sector-specific efforts. We also expect that efforts to implement the broader "cyber security review" regime that PRC government officials proposed (see our September 2014 client alert) will continue.

At this stage, it is unclear to what extent the detailed provisions of the Guideline and Catalogue in respect of the banking industry will guide future, more generally applicable legislation. Many of the sub-categories of products identified in the Catalogue are rather generic, and many of the criteria applied to those categories might easily be adopted in other sectors or in a broader cybersecurity review regime. At the least, it is not difficult to see the same arguments that were made for imposing the restrictions on the banking industry being made in respect of some other industries, and so we anticipate that the discussions and lobbying in regard to the Guideline and Catalogue that are currently underway will have ramifications beyond the banking sector.

WHAT THIS MEANS – NEXT STEPS FOR FITCS

The rather vague and open-ended language used in the Guideline and Catalogue makes it difficult for FITCs to plan ahead. However, it is possible to identify several steps that FITCs will need to consider:

(i) ***Assess the risk***. FITCs will need to review the products and services they offer to banks in China in order to assess and quantify the risks inherent in complying with the Guideline and Catalogue (for example, the IPR risks involved with disclosing sensitive source code or the security risks inherent in replacing software with indigenously sourced alternatives).

(ii) ***Assess the costs of localizing***. FITCs supplying almost every category of IT hardware and software listed in the Catalogue are required to operate R&D and service centers within China. Many FITCs will need to establish new PRC subsidiaries or repurpose their existing onshore affiliates in order to comply with this requirement. Doing so may require a material investment in capital and management time.

(iii) ***Assess the market***. FITCs will need to consider whether the value of the China banking market justifies the risk and costs identified under steps (i) and (ii). It may be that the banking sector constitutes a relatively small market segment for many FITCs. The cost-benefit analysis would look very different if the rules are generalized to other industries.

(iv) ***Identify procedures***. FITCs will need to identify the procedures involved in qualifying their products and services with CBRC and other relevant regulators. Some of these procedures already exist, and FITCs should seek advice from specialist, experienced counsel. Other procedures (for example, filing source code with CBRC) have not yet been established, and it may be sensible for FITCs to consider working with trade associations (see below).

(v) ***Consider forking***. In order to comply with the source code disclosure, indigenous innovation, and other requirements, we anticipate that some FITC vendors will seek to "fork" their product lines, creating specific versions for China that are likely, over time, to evolve away from the product lines used for the rest of the world.

(vi) ***Work with trade associations***. Many FITCs are working closely with the China chapters of international trade associations (for example, United States Information Technology Office, also known as "USITO") to stay abreast of the latest pronouncements from the CBRC and other relevant China regulators. In addition to disseminating information, such organizations have been seeking to engage the Chinese government in dialogue regarding how the Guideline and Catalogue will be interpreted and how best to implement key procedures (such as source code filing) in a manner that takes into account the legitimate concerns of FITCs.

Contact:

Paul D. McKenzie
(86) 10 5909 3366
pmckenzie@mofo.com

Gordon A. Milner
(852) 2585 0808
gmilner@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.