China Releases Draft Voluntary Information Security Standards for Public Comment

On 21 December 2016, China's National Information Security Standardization Technical Committee (NISSTC) released a set of draft information security standards (the "Standards") for public comment. The Standards include several individual documents covering: i) personal information, ii) cybersecurity, iii) big data, iv) certain devices, and vi) industrial control systems. Even though the Standards are voluntary and not legally binding, if passed they will provide useful guidance for organisations on how to fulfil their security obligations imposed by various laws including the Cybersecurity Law released last month.

Specifically, the draft *Personal Information Security Specification* (the "PI Specification") provides guidance on the collection, storage, use, transfer, and disclosure of personal information by certain organisations, namely those which process data sets involving more than ten thousand individuals within a consecutive 12-month period and have more than ten employees or have an annual revenue exceeding RMB 1 million. Many of the provisions in the PI Specification overlap with another voluntary guidance issued in 2013 (*Information Security Information Guidance on Protection of Personal Information of Public and Commercial Service Information System*) by, inter alia, defining key privacy concepts such as "sensitive personal information," "express consent," and "implied consent," all of which are currently absent in the mandatory PRC privacy laws and regulations.

The PI Specification makes significant progress by providing guidance in a number of areas.

First, the PI Specification, for the first time, adopts the EU concepts of "data subject" and "data controller," and also adopts the eight Organisation for Economic Co-operation and Development (OECD) privacy principles although it falls short on defining related concepts such as "data processor," and distinguishing the duties and obligations of the data controllers vs data processors.

Second, the PI Specification expands the scope of personal information developed in the 2013 Guidance to now cover information that may be identified by "all reasonable ways" that the data controller or any others may employ. Personal information includes information that can reveal a person's identity and other identifiable information (including biometrics and virtual identities such as social network nicknames and aliases), information gleaned from use of different services (including the content of telecommunications and social network postings, contact lists and correspondence), and personal services related information (including services logs, equipment identifiers, and location information). The scope of sensitive personal information has also been clarified and further expanded to include geo-location information and telephone records which are not typically recognised in other jurisdictions.

Third, the PI Specification requires that certain organisations have dedicated departments and appoint specific personnel to handle their information security. A recommendation has been included that a security risk assessment be conducted annually, whenever there is a change in privacy-related laws or a significant change occurs in the internal operation of the relevant business, or upon the occurrence of a security incident. Particular focus is placed on sensitive personal information which requires a separate system to document the collection, storage, access, and modification of such data. A security audit is required to track personal information and evaluate the efficacy of the security measures undertaken although there is no indication in the draft on the frequency of such an audit. The PI Specification includes a breach notification system which mandates reporting to the National Computer

Network Emergency Response Centre or relevant department within 24 hours of a data breach involving personal information of more than ten thousand individuals or sensitive personal information of more than 1,000 individuals. Data subjects should also be notified though no specific deadline is imposed on such notifications and they can be replaced by a public announcement if individual notifications are "difficult". There is no guidance on what "difficult notification" might mean.

Fourth, the PI Specification provides a model privacy notice. The model notice suggests that personal information may include personal information directly collected from a data subject or received from a third party as well as statistical data derived from such personal information. It is not clear in what way such data can amount to personal data. The model privacy notice further requires that the types of personal information to be collected be described clearly and that special notification be provided for sensitive personal information. There are special requirements that apply to online platforms which are required to disclose the potential risks involved in engaging in transactions on the platform and explain all security measures they adopt to safeguard the data they collect.

The draft *Implementation Guideline for Cybersecurity Classified Protection* (the "Cybersecurity Implementation Guideline") replaces the 2010 guideline previously issued by NISSTC. The Cybersecurity Implementation Guideline introduces a process to identify and classify the targets for specific cybersecurity protection focus such as big data, cloud computing platforms, products and services employing IoT, industrial control systems, and mobile Internet information systems. There is a special category for cloud computing platform services providers and cloud users of whom heightened cybersecurity protection will be expected. Large-scale cloud computing platforms, infrastructure providers and related services providers shall be deemed different protection targets subject to different security requirements. However, mobile internet information systems should be protected as one single system subject to a unified set of security protection strategies and measures.

The draft *Security Capability Requirements for Big Data Services* (the "Big Data Requirements") provides security guidance to big data service providers on the construction and operation of big data systems. The Big Data Requirements also contain guidance to third parties on how to conduct security assessments for big data services. The draft Big Data Requirements is the first comprehensive legal document in China focusing on big data security. Numerous 2-tiered security requirements are imposed, including 90 basic security requirements (30 are enhanced requirements), 214 security requirements for the management of big data lifecycle (92 are enhanced requirements), and 288 requirements for big data platform and application security (92 are enhanced requirements).

The draft *Testing and Evaluation Methods for the Security of Devices* provides standards for testing and evaluating devices such as printers, scanners, fax machines, and copy machines for purchasers and distributors.

The remaining three draft standards relate to industrial control systems—one of the emerging technologies—and cover areas such as risk assessment, vulnerability detection, and network monitoring.

The public comment period closes on 2 February, 2017. Comments can be posted on the NISSTC official website and will be collected by the NISSTC for review. Although the Standards throw some light on a number of areas they also cloud many issues by introducing new vague requirements (viz security audits; breach notifications to individuals) or concepts (statistical information). Clarification for these concepts and requirements can be sought through submissions to NISSTC during the consultation period.

Contact Us

For enquiries related to this Legal Update, please contact the following persons or your usual contact at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Xiaoyan Zhang
Counsel, (New York, USA)
T: +852 2843 2209
E: xiaoyan.zhang@mayerbrownjsm.com