WILMERHALE

# Cross-Border Data Flows Security Assessments in China

JUNE 8, 2017

China has issued for public comment draft standard-like guidelines to govern cross-border data flows to further implement China's heightened concern over national security and cybersecurity, as embodied in the National Security Law (2015), Cybersecurity Law (effective June 1, 2017) and related laws and regulations. These Guidelines, open to public comment through June 27, were formulated by Technical Committee 260 (TC260) and issued by the General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ) and the Standardization Administration of China (SAC). The Guidelines would apply to all Network Operators in China, including foreign-invested enterprises and providers of services to Networks. They would subject cross-border data flows covering a very wide range of subject matters to security assessments and privacy consents. If the Guidelines are adopted without extensive revision, they present a major challenge to the ability of companies and other entities involved in China to engage on a timely basis across borders in business and other activities not generally deemed to be national security-related. As such, the Guidelines threaten to undercut China's stated commitments to globalization.

**Purposes**

The Guidelines, termed the Information Security Technology—Guidelines for Data Cross-Border Transfer Security Assessment (the Guidelines), set forth the procedures, principal assessment concerns, and methods for cross-border data transfer security assessments. The Guidelines would be applicable to Network Operators for the conduct of security assessments of cross-border transfers of personal information and important data, and be applicable to industry regulators and supervisors to guide and supervise Network Operators in their security assessments of cross-border transfers of personal information and important data [Article 1]. Network Operators are broadly defined as the owners and operators of networks as well as providers of services to networks [Article 3.1]. Networks are defined in the Cybersecurity Law as the systems comprising computers or other information terminals and equipment that collect, store, transmit, exchange and process information under specified rules and procedures.

Data under the Guidelines is defined as personal information and important data in an electronic form collected and generated in the course of operations in China [Article 3.2]. Network Operators would be required to follow the Guidelines in the conduct of security assessments of personal information and important data to be transferred overseas, discover security issues and risks, and

take prompt action to prevent the flow of personal information overseas without consent that may compromise the lawful rights of the subjects of personal information; and to prevent important state data from being stored overseas without a security assessment and approval by the applicable regulators to prevent adverse impacts on national security [Preamble]. “Overseas” would include the Special Administrative Regions of Hong Kong and Macau. The Cyberspace Administration of China (CAC), industry regulators and supervisory departments may also take the Guidelines as reference for security assessments conducted in their respective spheres of responsibility [Article 1].

**Definitions**

The Guidelines consist of five articles that encompass the scope of application, definitions, assessment procedures and principal assessment concerns, together with lengthy Appendices A and B which define important data across 28 industry sectors and security assessment methods for outbound data transfer risks.

The Guidelines define such terms as Important Data, Sensitive Personal Information, Data Cross-Border Transfer (sic), Provide [Provision] and Data Desensitization. Important Data includes data related to national security, economic development, and societal and public interests, as further detailed in the 28 industry sectors listed in Appendix A. Cross-border data transfers would not include overseas data transiting China without being modified, processed or disposed of in China [Article 3.6]. “Provision” would include both voluntary data provision overseas by Network Operators as well as provision overseas by the users of product and service functions provided by Network Operators. Network Operators providing data that has previously been disclosed to the public in accordance with law would not be deemed Provision [Article 3.8]. Note here that “in accordance with law” is not equivalent to “in the public domain” as information in the public domain that is subsequently deemed to have been improperly made public would be subject to a security assessment.

**Assessment Procedures and Principal Assessment Concerns**

Network Operators would be obligated to conduct a security assessment when the products and/or services involve data provision to overseas institutions, organizations or individuals, or when there are relatively large changes in the purpose, scope, type or quantity of the products/services for which outbound data transfer security assessments have previously been conducted, or when there are changes in the data recipients, or in the event of major security incidents [Article 4.1]. Network Operators would be required to formulate outbound data transfer plans to specify the purpose, scope, type, scale, information system, country in transit, basic conditions of data recipients and countries/regions where they are located, and security control measures before conducting a data transfer [Article 4.2].

Principal assessment concerns include the plan's legality, propriety and risk controllability [Article 4.3]. Outbound data transfers will be required to satisfy specific legal and proper requirements in effect at the time of transfer. The legal requirements are: (i) not prohibited by law or regulation from outbound transfer; (ii) in compliance with international treaties or agreements; (iii) consented to by the subject of personal information, except in emergency circumstances when the subject's life or

property are endangered; or (iv) not prohibited from outbound transfer by the cybersecurity, public security or state security departments in accordance with law. Proper requirements to be satisfied at the time of transfer are: (i) implementation of essential measures by the Network Operator acting within its authorized scope of business; (ii) compliance with the obligations of the underlying contracts; (iii) compliance with law; (iv) assistance with the administration of justice; and (v) other requirements to safeguard cyber sovereignty, national security, societal and public interests, and to protect the lawful rights of citizens. Requirement (v) in particular grants the authority broad latitude to restrict cross-border data transfers [Article 5.1].

Assessments of risk controllability would need to give consideration to data attributes and the potential for occurrence of security incidents after outbound transfer, cross-border data transferors' technological and management capability, data recipients' security protection capability, and the political and legal environment in countries/regions where the data recipients are located [Article 5.2.6]. The volume, category and scope of data and technical processing are all principal concerns. Personal information may have a derivative value after data collection when a numerical threshold of subjects of personal information is exceeded [Article 5.2.2.2]. Categories of important data to be assessed include those involving nuclear facilities, chemical biology, defense and the military industry, public health, large projects, the marine environment and sensitive geographical data, critical information infrastructure (CII) system gaps, and more [Article 5.2.3.1]. Appendix A sets out the scope of important data for 28 industrial sectors, including oil & gas, coal, petrochemicals, nonferrous metals, steel, geography, power, communications, electronic information, public health, postal express mail, finance, food and drugs, statistics, meteorology, environmental protection, broadcast media, marine environment, and e-commerce.

If the requirements for legality and propriety or risk controllability are not satisfied, Network Operators may modify their outbound transfer plans or lower the risks of outbound transfers by streaming the data content, reducing the level of sensitivity, restricting disposition by the data recipient, or other means [Article 4.6].

www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf

## *Authors*


### Lester Ross

**PARTNER**

Partner-in-Charge, Beijing Office

lester.ross@wilmerhale.com

+86 10 5901 6588