PILLAR LEGAL

China Releases Proposed Guidelines for Cross-Border Data Transfer Security Assessment

CHINA REGULATION WATCH[1]
July 7, 2017

By: Greg Pilarowski | Charles Yu | Samuel Gintel

On May 27, 2017, the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会) published for public comment a draft of the proposed Guidelines for Cross-Border Data Transfer Security Assessment (数据出境安全评估指南) (the "Draft Security Assessment Guidelines"). The Draft Security Assessment Guidelines, if adopted, provide an analytical framework for determining the kind of security assessment(s) that should be conducted, and the standards that apply to such security assessment(s), in connection with a transfer of Personal Information (as defined below) and/or Critical Data (as defined below) out of China (a "Cross-Border Data Transfer").

These Draft Security Assessment Guidelines follow other laws and regulations regarding the restriction of Cross-Border Data Transfers that have either recently come into effect or are still in the proposal phase in China, including but not limited to the Cyber Security Law of the People's Republic of China (中华人民共和国网络安全法), issued by the Standing Committee of the National People's Congress (全国人民代表大会常务委员会) on November 7, 2016, which came into effect on June 1, 2017 (the "Cyber Security Law"), and the Proposed Measures for Security Assessment of Transferring Personal Information and Critical Data Overseas (个人信息和重要数据出境安全评估办法), issued by the Cyberspace Administration of China, also known as the State Internet Information Office (国家互联网信息办公室) (the "CAC"), on April 11, 2017 (the "Draft Data Transfer Measures").[2] Although both the Cyber Security Law and the Draft Data Transfer Measures require security assessments to be performed before Personal Information and Critical Data collected within China can be legally transferred out of China,[3] neither of those rules provide clear guidelines on how such security assessments shall be conducted.

The primary purpose of the Draft Security Assessment Guidelines is to provide such guidelines by setting forth the relevant processes and standards that, if adopted, will apply when conducting security assessments before transmitting Personal Information and Critical Data outside of China. The Draft Security Assessment Guidelines also clarify and define certain vague terms used in the

[1] This China Regulation Watch is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This China Regulation Watch may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-474-3258 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: greg@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Click here to read more about the Draft Data Transfer Measures.

[3] See Section 37 of the Cyber Security Laws, and Section 2 of the Draft Data Transfer Measures.

Cyber Security Law and the Draft Data Transfer Measures, including the terms "Personal Information" and "Critical Data".

Although the Draft Security Assessment Guidelines are not yet final, they provide insight into how security assessments in connection with Cross-Border Data Transfers are likely to be conducted. Because the Draft Security Assessment Guidelines essentially supplement the Draft Data Transfer Measures by providing details into how certain provisions of the Draft Data Transfer Measures are to be implemented, however, changes by the CAC to the Draft Data Transfer Measures when finalized will likely entail corresponding changes to the Draft Security Assessment Guidelines.

1. Scope of the Draft Security Assessment Guidelines.

Pursuant to the Draft Data Transfer Measures, prior to a Cross-Border Data Transfer, an internet operator must conduct a security self-evaluation assessment (a "Self-Assessment").[4] In addition, under certain circumstances, an internet operator must submit an application to the relevant primary industry regulator for a security assessment in connection with a proposed Cross-Border Data Transfer (a "Regulator Assessment").[5] The security assessment procedures and standards set forth in the Draft Security Assessment Guidelines, if adopted, shall apply to both Self-Assessments and Regulator Assessments.[6]

Because the rules requiring Self-Assessments and Regulator Assessments, if adopted, would apply to Cross-Border Data Transfers by internet operators, the scope of the term "internet operator" is relevant in determining who is subject to such rules. Pursuant to both the Draft Data Transfer Measures and the Draft Security Assessment Guidelines, "internet operator" is defined broadly to include "all network owners, network managers, and internet service providers."[7] We understand this broad language to include all companies, individuals and organizations that collect Personal Information and/or Critical Data through the internet. Under the Cyber Security Law, a security assessment is only required in connection with a Cross-Border Data Transfer if the relevant internet operator operates a critical information infrastructure.[8] The Draft Security Assessment Guidelines, however, broaden the security assessment requirement to apply to all internet operators regardless of whether such internet operators operate critical information infrastructures.

[4] See Section 8 of the Draft Data Transfer Measures.
[5] See Section 9 of the Draft Data Transfer Measures. Pursuant to Section 9 of the Draft Data Transfer Measures, a Regulator Assessment shall be conducted, if the data proposed to be transferred out of China: (i) includes the Personal Information of more than 500,000 persons; (ii) has a storage size that exceeds 1,000 gigabytes; (iii) includes information related to nuclear facilities, chemical biology, national defense, military, human health, large-scale construction projects, marine environment or geographic information about sensitive locations; (iv) includes information relating to system loopholes or security protection measures for critical information infrastructure; (v) originates from internet operators who operate critical information infrastructure; and (vi) has the potential to affect national security or societal public interests, and the respective primary regulators believe it is necessary to conduct a security assessment with respect to such data.
[6] See Section 1 of the Draft Security Assessment Guidelines.
[7] See Section 3.1 of the Draft Security Assessment Guidelines.
[8] See Section 37 of the Cyber Security Laws.

2. Definition of Personal Information and Critical Data.

As used in the Draft Security Assessment Guidelines:

(1) "Personal Information" means all information that can be used on its own or together with other information to determine the identity of a natural person, including an individual's name, date of birth, identification card number, contact information, biometric data, address, online account numbers and passwords, financial information, and location and behavior information.

The Draft Security Assessment Guidelines expanded the scope of "Personal Information" to also include the last part of the definition, "online account numbers and passwords, financial information, and location and behavior information", which was not included in the definition of "Personal Information" in the Draft Data Transfer Measures that was recently published for public comment.[9]

(2) "Critical Data" means data that is very closely related to China's national security, economic development or societal public interests.[10] Although this definition is very broad, Annex A of the Draft Security Assessment Guidelines provides a detailed breakdown of 28 industry sectors, the primary regulators of each such industry sector and the Critical Data relevant in the context of each such industry sector. According to Annex A of the Draft Security Assessment Guidelines, Critical Data tends to be relevant in the following industries: energy, manufacturing, military, nuclear, geography, demography and the environment. Certain data related to e-commerce, however, will also be regarded as Critical Data if, for example, such data includes registration information of users, whether or not such users are individuals or entities, users' credit records and credit evaluation information, individual users' consumption habits and preferences and entity users' business operation data.[11]

3. Security Assessment Procedure.

In order to conduct a security assessment pursuant to the Draft Security Assessment Guidelines, an internet operator shall prepare a plan for the proposed Cross-Border Data Transfer (a "Plan"), which shall specify: (i) the purpose, scope, type and scale of the Cross-Border Data Transfer; (ii) the information system relevant to such Cross-Border Data Transfer; (iii) the countries and regions that act as data intermediate transit points for such Cross-Border Data Transfer (if any); (iv) basic information about the identity of the recipient(s) of the data and countr(ies)/region(s) where such recipient(s) are located; and (v) the data safety control measures to be taken by such internet operator.[12]

Once an internet operator has prepared a Plan, the internet operator will conduct a security assessment for the Cross-Border Data Transfer in accordance with procedures and standards set forth in the Draft Security Assessment Guidelines. First, the legitimacy of such Cross-Border

[9] See Section 17 of the Draft Data Transfer Measures.
[10] See Section 3.5 of the Draft Security Assessment Guidelines.
[11] See Section A.27 of Annex A of the Draft Security Assessment Guidelines.
[12] See Section 4.2 of the Draft Security Assessment Guidelines.

Data Transfer will be evaluated. If such Cross-Border Data Transfer fails to comply with the legitimacy requirements, which are described further below, such Cross-Border Data Transfer will not be permitted.[13]

If such Cross-Border Data Transfer satisfies the legitimacy requirements, then the risk levels associated with such Cross-Border Data Transfer will be evaluated. Pursuant to the Draft Security Assessment Guidelines, the risk levels of a Cross-Border Data Transfer are to be categorized as either low, medium, high or very high. If the risk level of a Cross-Border Data Transfer is categorized as high or very high, the Personal Information and/or Critical Data associated with such Cross-Border Data Transfer shall not be transferred out of China.[14]

Internet operators must prepare reports with respect to each of their security assessments, and such reports must be kept for at least five (5) years.[15] A flow chart depiction of the security assessment procedure is set forth below in Schedule I.

4. Principal Assessment Factors.

As indicated in connection with the security assessment procedure described above, the two principal assessment factors for a Cross-Border Data Transfer are (i) the legitimacy requirement and (ii) the risk levels.[16]

(1) Legitimacy Requirement. Pursuant to the Draft Security Assessment Guidelines, each Cross-Border Data Transfer must be legal and reasonable.[17]

In order to be legal, a Cross-Border Data Transfer shall: (i) not be a transfer prohibited by relevant laws and regulations; (ii) be in compliance with international treaties or agreements of which China is a signatory; (iii) only be carried if the relevant consent of the owner of any Personal Information contained in such Cross-Border Data Transfer has been obtained, except in emergency circumstances when the subject's life or property are endangered; and (iv) not be prohibited by the CAC or the state public security department.[18]

In order to be reasonable, a Cross-Border Data Transfer shall be necessary: (i) for the relevant internet operator to conduct its ordinary business within its authorized business scope; (ii) to perform a contract; (iii) to undertake obligations required by law; (iv) for judicial assistance; or (v) to safeguard cyber sovereignty, national security, societal and public interests, and to protect the lawful rights of citizens.[19]

(2) Risk Level. Pursuant to the Draft Security Assessment Guidelines, the risk level of a Cross-Border Data Transfer shall be determined by (i) the characteristic of the data proposed to

[13] See Section 4.3 of the Draft Security Assessment Guidelines.
[14] See Section 4.4 of the Draft Security Assessment Guidelines
[15] See Section 4.5 of the Draft Security Assessment Guidelines.
[16] See Section 4.3 of the Draft Security Assessment Guidelines.
[17] See Section 5.1 of the Draft Security Assessment Guidelines.
[18] See Section 5.1(a) of the Draft Security Assessment Guidelines.
[19] See Section 5.1(a) of the Draft Security Assessment Guidelines.

be transferred and (ii) the possibility of a security incident occurring in connection with such Cross-Border Data Transfer.[20]

(i) Characteristic of Data. The table below summarizes the characteristics of the Personal Information and/or Critical Data that are considered in connection with determining the risk level associated with a proposed Cross-Border Data Transfer.

Personal Information	**Critical Data**
- Volume of the data, - Scope of the data, - Category of the data, - Amount of "Sensitive Personal Information" included,[21] and - The technical processes used to protect the confidential information.	- Volume of the data, - Scope of the data, - Category of the data, - The technical processes used to protect the confidential information.

When evaluating the scope of the Personal Information and/or Critical Data that is proposed to be transferred out of China, the "minimum scope principal" shall apply, which requires the following conditions to be satisfied:[22]

(a) Transferring Personal Information and/or Critical Data out of China must be necessary for conducting an internet operator's ordinary business.

(b) The frequency of transferring Personal Information and/or Critical Data out of China shall not exceed the necessary frequency required to conduct the ordinary business of the internet operator.

(c) The volume of Personal Information and/or Critical Data transferred out of China in each particular instance shall not exceed the volume that is necessary to conduct the ordinary business of the internet operator.

The characteristics of Personal Information and/or Critical Data shall be used to determine the risk level associated with such Cross-Border Data Transfer based on a mechanism and scale that is described further in Annex B of the Draft Security Assessment Guidelines (the "Impact Level").[23] The Impact Level ranges on a scale from level 1 to level 5, with level 1 corresponding

[20] See Section 5.2.1 of the Draft Security Assessment Guidelines.
[21] Pursuant to Section 3.4 of the Draft Security Assessment Guidelines, "Sensitive Personal Information" is proposed to mean Personal Information which, if divulged, illegally provided to a third party or abused, could pose a threat to the safety of persons or property, damage the reputations or physical or mental health of individuals, or lead to unfair discrimination.
[22] Section 5.2.2.3 and Section 5.2.3.3 of the Draft Security Assessment Guidelines.
[23] See Section B.1 and Section B.2 of Annex B of the Draft Security Assessment Guidelines.

to the lowest level of risk, and level 5 corresponding to the highest level of risk, associated with such Cross-Border Data Transfer.

In order to determine the Impact Level for a Cross-Border Data Transfer of Personal Information, the default Impact Level ranges from level 1 to level 3 depending on how much "sensitive personal information" is included in the Personal Information that is proposed to be transferred out of China.[24] The Impact Level for a Cross-Border Data Transfer of Personal Information will increase one level if (i) such transfer includes the Personal Information of more than 500,000 persons cumulatively in one year, or (ii) the transfer of such Personal Information fails to comply with the "minimum scope principle". In addition, the Impact Level for a Cross-Border Data Transfer of Personal Information will decline one level if security measures have been implemented to protect confidential information.[25]

In order to determine the Impact Level for a Cross-Border Data Transfer of Critical Data, the default Impact Level is level 4. The Impact Level for a Cross-Border Data Transfer of Critical Data will increase one level, if (i) the storage size of the Critical Data exceeds 1,000 gigabytes cumulatively in one year, or (ii) the transfer of the Critical Data fails to comply with the "minimum scope principle". In addition, the Impact Level for a Cross-Border Data Transfer of Critical Data will decline one level if security measures have been implemented to protect the confidential information.[26]

(ii) Security Incident Risk. When evaluating the possibility of a security incident occurring in connection with a Cross-Border Data Transfer (the "Security Incident Risk"), the following key factors will be considered based on the mechanism as further described in Annex B of the Draft Security Assessment Guidelines and below:[27]

(a) The technological and management capability of the data transferor;

(b) The security protection capability of the data recipient; and

(c) The political and legal environment in the countries/regions where the data recipients are located.

The Security Incident Risk ranges on a scale from level 1 to level 3 depending on the key factors described above, with level 1 corresponding to the lowest level of risk, and level 3 corresponding to the highest level of risk, of a security incident occurring.

[24] See Section B.1 of Annex B of the Draft Security Assessment Guidelines. Pursuant to Section B.1 of the Annex B of the Draft Security Assessment Guidelines, (i) if there is no sensitive personal information included, the basic Impact Level shall be level 1, (ii) if only a minority of the data includes sensitive personal information included, the basic Impact Level shall be level 2, and (iii) if there is a majority of such Personal Information includes sensitive personal information, the basic Impact Level shall be level 3.
[25] See Section B.1 of Annex B of the Draft Security Assessment Guidelines.
[26] See Section B.2 of Annex B of the Draft Security Assessment Guidelines.
[27] See Section 5.2.1(b) of the Draft Security Assessment Guidelines, and Section B.3 of Annex B of the Draft Security Assessment Guidelines.

The table below shows how the Impact Level and the Security Incident Risk are both analyzed together to determine the risk level associated with a Cross-Border Data Transfer.[28]

		Security Incident Risk		
		1	2	3
Impact Level	≥5	High	Very High	Very High
	4	Medium	High	High
	3	Low	Medium	High
	2	Low	Medium	Medium
	1	Low	Low	Medium

[28] Section B.4 of Annex B of the Draft Security Assessment Guidelines.

PILLAR LEGAL

SCHEDULE I

SECURITY ASSESSMENT PROCEDURE