China Seeks Comments on Updated Draft of Cross-Border Data Transfer Security Assessment Standard

August 31, 2017

Data Privacy and Cybersecurity

On August 31, 2017, China's National Information Security Standardization Technical Committee ("NISSTC"), a standard-setting committee jointly supervised by the Standardization Administration of China ("SAC") and the Cyberspace Administration of China ("CAC"), released an updated draft of the *Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment* for public comment (the "draft Standard") (official Chinese version available here.) The comment period for this draft national standard ends on October 13, 2017.

A previous version of the draft Standard was released for public comment on May 27, 2017. (Covington's blog post on the previous draft is available here.)

Once adopted, this standard will be part of a comprehensive regime governing China's cross-border data transfers. It supplements the draft implementing regulation issued by the CAC in May of this year, *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data* ("the Measures"). (Covington's alert on the Measures is available here.) Although not legally binding and lacking the force of law, this draft Standard is expected to provide important guidance to companies with respect to the security assessment of their cross border data flows. The result of such assessment will in turn determine whether a company's cross border data transfers can continue, or have to be adjusted, or will be prohibited altogether.

This alert summarizes the key changes from the previous draft and explains the potential impact on companies' operations in China.

Definition of Cross-Border Data Transfer

The draft Standard inserts a new definition of "data cross-border transfer," which is "one-time or continuous provision of personal information or important data to entities outside of China by way of direct data provision, transactions or through provision of services or products by network operators." The draft Standard also clarifies that the following actions should be considered cross-border data transfers:

- providing data to entities located in China but that (i) are not subject to Chinese jurisdiction or (ii) are not registered in China;

- foreign entities, organizations, or individuals accessing data stored in China (except for accessing public information or webpages); and
- transferring data collected or generated in the course of operations within China to affiliated group companies outside of China.

Note that consistent with the previous draft and the draft Measures, the draft Standard extends cross-border transfer requirements to "network operators," a much broader term than "operators of critical information infrastructure" ("CII operators"). "Network operator" is defined to include "owners and managers of networks, as well as network service providers." The draft Measures provide that when network operators transfer abroad personal information and important data collected or generated in the course of operations within China, a security assessment should be conducted. The draft Standard follows the same approach.

The draft Standard further explains that the following two types of transfer will not be considered to be cross-border data transfers:

- transfer of data *through* China, if such data is not collected or generated in China and not changed or processed in China;
- transfer of data that is not collected or generated in China, even though such data is stored or processed in China.

No change has been made to Annex A, which provides guidance on the identification of "important data" from the previous draft.

Security Self-Assessment

The draft Standard requires network operators to conduct a security self-assessment annually and initiate the self-assessment if any of the following circumstances rises:

- if cross-border data transfers (as defined above) occur;
- if a CII operator is transferring data across borders;
- although the self-assessment has been completed, if the purpose, scope, and type of the cross-border transfer are changed significantly, the data recipient is changed, or a serious security incident has occurred;
- as required by sector regulators.

Note that the customer of cloud service should be responsible for the self-assessment if it requests cross-border data transfers. If a transfer is not initiated by a customer, but by the cloud provider itself, the cloud provider should be responsible for the self-assessment.

According to the draft Standard, network operators are required to prepare a self-assessment report after the completion of the security self-assessment. This report should be retained for at least two years and network operators have an affirmative obligation to report the results of their self-assessment to the sector regulators or CAC under the following circumstances:

- the self-assessment is conducted by CII operators;
- the quantity of personal information that is transferred within one year meets the threshold set by the CAC and sector regulators;

- data regarding "nuclear facilities, chemical biology, national defense or military, population and health care, etc." and data related to "large-scale engineering activities, marine environment, and sensitive geographic information," and other important data;
- data related to cybersecurity information of CII operators, such as their system vulnerabilities or security measures;
- other transfers that may potentially affect China's national security, economic development, and public interests.

Note that the previous draft mentioned transfer of personal information of over 500,000 Chinese citizens within one year as one of the thresholds for reporting a network operator's self-assessment to the regulators. This draft removes that number and presumably leaves the criteria for the regulators to decide later.

Regulators' Security Assessment

Under certain circumstances, CAC or sector regulators may launch a security assessment on its own initiative. In addition to circumstances that would trigger a network operator's reporting obligation (described above), the following circumstances may also trigger a regulator's assessment:

- if data transfers receive a large amount of complaints from users;
- if the security assessment (of transfers by a network operator) is suggested by national industry associations;
- other transfers determined by CAC or sector regulators as necessary to review.

Note that if multiple network operators are involved in the transfers (such as in the case of cloud service providers), the regulator which will conduct the security assessment will be the regulator that has jurisdiction over the network operator which requested the transfer.

Regulators are required to formulate an assessment plan and establish a working group to carry out the security assessment by way of "remote testing" and "on-site inspection." The working group should prepare an assessment report discussing the assessment results, including the material risks of transfers and mitigation or adjustment recommendations (if any). Such report should be reviewed by an expert committee organized by CAC or sector regulators and the committee will advise CAC or sector regulators on whether the proposed data transfer should be approved. CAC or sector regulators will make the final decision based on the assessment report prepared by the working group and the suggestions from the expert committee.

A flowchart of regulators' security assessment is attached as an annex to this alert.

Substantive Criteria for the Security Assessment

The draft Standard instructs both network operators and regulators to evaluate (i) whether the transfers are lawful, legitimate, and necessary and (ii) risks associated with the transfers.

As a threshold requirement, the transfers at issue should be "lawful", "legitimate," and "necessary":

- The lawfulness of a transfer depends, among other things, on whether laws or regulations explicitly prohibit the transfer or whether the transfer is prohibited by the CAC or public security or national security agencies.
- If consent has been obtained for transfers of personal information, the transfers are legitimate, unless under exceptional circumstances where transfers would be "necessitated by an emergency that could endanger the lives and property of [Chinese] citizens."
    - Consent will be deemed to be obtained if (i) the data subject dials international calls, sends international emails, or engages in international transactions; and (ii) the data to be transferred is legally disclosed to the public.
- Transfers for "the internal business operation of a company" and for "fulfilling business contracts," among other reasons, would qualify as necessary.

As the second step, network operators and the regulators should focus on the risks associated with the transfers. The assessment is required to focus on two elements:

- features of the data being transferred, including types, quantity, scope, sensitivity and technical processing status;
- likelihood of security incidents and the level of impact of such incidents.

For the second element, the draft Standard further lists over 15 risk factors, including ones related to a data controller's data protection program, the data recipient's level of protection, and the country to which the data will be sent. For example, the draft Standard contemplates that the transfer of sensitive personal information would have a higher risk level than the transfer of other personal information. Regulators will also assess a company's data protection program from two perspectives: data protection governance and technical measures used to protect the data. The absence of any data protection practices may be deemed as increasing the overall risk of the transfers. Finally, regulators consider a review of the data recipient's security practices and the "political and legal environment" of the country or region in which the data recipient is located to be necessary in order to assess the overall risk of the transfer.

Risk factors identified in the draft Standard will be used to evaluate a company's data transfer practices. For each risk factor, the regulator will assign a risk level. Once all risk factors are assessed, a regulator can decide the overall risk level of the transfers. If the overall risk level is low, such transfers should be allowed to continue. If the risk level is high, a company may be ordered to stop the transfers and step up its security measure before it can resume the transfers.

For more information on this alert, please contact any of the below Covington lawyers:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com

Flowchart of Regulators' Security Assessment