HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

Han Kun Newsletter

Issue 185 (9th edition of 2022)

Legal Updates

1. A Brief Overview of the Draft Amendment to the Cybersecurity Law
2. CAC Issues Guidelines for Data Export Security Assessment

1. A Brief Overview of the Draft Amendment to the Cybersecurity Law

Authors: Kevin DUAN | Kemeng CAI | Jin JIN

Introduction

On September 14, 2022, the Cyberspace Administration of China (the "**CAC**") released an exposure draft of the *Decision on Amending the Cybersecurity Law of the People's Republic of China (Draft for Comment)* (the "**Draft**"). In general, the Draft would impose more stringent legal liabilities for certain violations of the Cybersecurity Law (the "**CSL**") and systematically consolidate and unify penalties for violating security protection obligations relating to network operations, network information, critical information infrastructure ("**CII**"), and personal information. The Draft would also coordinate with the Personal Information Protection Law (the "**PIPL**"), the Data Security Law, and other new laws. We briefly summarize the key points of the Draft below.

Stricter legal liabilities for violating network operation security obligations

The Draft would consolidate and unify liabilities for violating various general provisions on network operation security, including security protection obligations required by the Multi-level Protection Scheme, obligations to develop and implement emergency plans for network security incidents, and obligations to provide continuous security maintenance of products and services. Compared to the current CSL, the Draft would supplement the penalties for violating Article 23, which requires security certification or security testing for critical network equipment and special cybersecurity products. Notably, liabilities for violating these provisions would be made more stringent. The Draft echoes Article 66 of the PIPL by raising the maximum fine for personal information processors to RMB 50 million or five percent of their previous year's turnover. The Draft would also raise the maximum fines for persons directly liable to up to 1 million yuan and add the penalty of prohibiting such persons from taking management or key cybersecurity protection positions.

Related articles	Liabilities under the CSL	Liabilities under the Draft
Article 21 The State adopts Multi-level Protection Scheme, under which network operators are required to perform the following obligations of security protection to ensure that the network is free from interference, disruption or unauthorized access, and prevent network data from being disclosed, stolen or tampered: 1. Formulating internal security management systems and operation instructions to determine the person in charge	**【Liabilities for violating network operation security】** The competent authority shall warn such operator and order it to make rectifications. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 5,000	**【Liabilities for violating network security protection】** The competent authority shall warn such operator and order it to make rectifications. A fine **of up to 1 million yuan** shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as

Related articles	Liabilities under the CSL	Liabilities under the Draft
of cybersecurity and define accountabilities for cybersecurity; 2. Taking technical measures to prevent computer virus, network attacks, network intrusions and other activities that endanger cybersecurity; 3. Taking technical measures to monitor and record network operation and cybersecurity events, and maintaining the cyber-related logs for no less than six months as required; 4. Taking such measures as data classification, and backup and encryption of important data, etc.; and 5. Performing other obligations provided for in relevant laws and administrative regulations.	to 50,000 yuan shall be imposed on the supervisor directly in charge.	suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons. For any illegal act specified in the preceding paragraph with particularly serious circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose a fine **ranging from 1 million to 50 million yuan or not more than 5% of its turnover in the previous year**, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine **ranging from 100,000 yuan to 1 million yuan** shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to **prohibit the said persons from taking positions of directors, supervisors, senior executives or key cybersecurity and network operation**
Article 25 Network operators shall develop an emergency plan for cybersecurity events to promptly respond to such security risks as system bug, computer virus, network attacks and intrusions. For an event that threatens cybersecurity, the operator concerned shall forthwith initiate the emergency plan, take corresponding remedial actions, and report as required such event to competent authority concerned.		
Article 33 A critical information infrastructure shall be developed with the capacity to support the steady and continuous business operation, and technical security measures shall be planned, established and put into use simultaneously.	**【Liabilities for CII who violates network operation security obligations】** The competent authority shall warn such operator and order it to make rectifications. A fine ranging from 100,000 yuan to 1 million yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000	
Article 34 In addition to those provided in Article 20 hereof, the operator of a critical information infrastructure shall also fulfill obligations of security protection		

Related articles	Liabilities under the CSL	Liabilities under the Draft
as follows: 1. Set up a dedicated security management body and designate a person in charge, and review the security backgrounds of the said person and those in key positions; 2. Provide practitioners with regular cybersecurity education, technical training and skill assessment; 3. Make disaster recovery backup of important systems and databases; 4. Work out an emergency plan for cybersecurity events and carry out drills regularly; and 5. Perform other obligations provided for in relevant laws and administrative regulations.	yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.	**positions.**
Article 36 The operator of a critical information infrastructure shall, in purchase of network products and services, enter into an agreement with the product/service provider in which obligations and responsibilities of security and confidentiality shall be specified.		
Article 38 The operator of a critical information infrastructure shall conduct, by itself or entrusting a cybersecurity service provider, examination and assessment of its cybersecurity and potential risks at least once a year, and submit the examination and assessment results as well as improvement measures to the competent authorities in charge of the security of the critical information infrastructure.		
Article 22 Paragraph 1 & 2 Network products and services shall satisfy the mandatory requirements set forth in applicable national standards. Any provider of network products or services shall not install malwares. For any risk	**【Liabilities for violating network product and service security obligations】** The competent authority shall give a warning and an order of rectification. A fine ranging	

Related articles	Liabilities under the CSL	Liabilities under the Draft
such as security defect or bug that is found, the provider concerned shall, as required, immediately take remedial actions, inform the users of the said risk, and report the case to the competent authority. **A provider of network products or services shall also provide consistent security maintenance for its products or services. Such maintenance shall not be discontinued within the prescribed term or the term agreed upon by the parties thereto.**	from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.	
~~**Article 48 Paragraph 1 Electronic information sent and applications provided by any individual and organization shall be free of malwares and information that are prohibited by laws and administrative regulations from release or transmission.**~~		
Article 24 Network operators shall require the users to provide their real identity information when signing agreements or confirmations on the provision of such services as network access, domain name registration, fixed phone and mobile phone network access, or information release and instant communication. In case that a user does not provide his/her real identity information, no network operator may provide related services for the user.	**【Liabilities for violating user identification obligation】** The competent authority shall order such operator to make rectifications. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or of severe circumstance, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be imposed by competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable	

Related articles	Liabilities under the CSL	Liabilities under the Draft
	persons.	
Article 26 Activities such as cybersecurity authentication, testing, and risk assessment, and releasing of cybersecurity information such as system bug, computer virus, network attacks and intrusions shall be carried out in compliance with applicable regulations of the State.	**【Liabilities for illegally operating network service】** The competent authority shall warn such operator and order it to make rectifications. A fine of ranging from 10,000 yuan to 100,000 yuan shall be imposed in case of refusal to make rectifications or severe circumstance, and further penalties such as suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by the competent authority. A fine ranging from 5,000 yuan to 50,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.	
Article 23 Under the compulsory requirements set forth in national standards, critical network equipment and special-purpose cybersecurity products shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organization. CAC shall work with departments concerned of the State Council to formulate and release a catalogue of critical network equipment and special-purpose cybersecurity products, and promote mutual recognition of security certificate and security test results for the avoidance of repeated certification and tests.	**Liabilities not stipulated**	
Article 28 Network operators shall provide public security organs and	**【Liabilities for refusing to assist in maintaining**	

Related articles	Liabilities under the CSL	Liabilities under the Draft
national security authorities with technical support and assistance in their attempts to safeguard national security and investigate into crimes.	**national security and investigating into crimes】** Shall be warned and ordered by the competent authority to make rectifications. A fine of ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.	
Article 27 No individual or organization may engage in activities that threaten cybersecurity such as unlawful intrusion into others' networks, interfering with the normal functions of others' network and stealing network data, provide programs or tools for such intrusions, interference or stealing, or provide any assistance such as technical support, advertisement, payment or settlement for any other person if the individual or organization is fully aware that such person engages in an activity endangering cybersecurity.	**【Liabilities for threatening network security】** While not constituting a crime, it shall be subject to confiscation of illegal earnings and detention of less than 5 days by the public security authority and a fine ranging from 50,000 yuan to 500,000 yuan. Severe violation in this regard shall be subject to a detention of above 5 days but below 15 days and a fine ranging from 100,000 yuan to 1 million yuan. Any organization the conduct mentioned in the preceding paragraph shall be subject to confiscation of illegal earnings by the public security authority and a fine ranging from 100,000 yuan to 1 million yuan. The supervisor directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph. Any person who violates Article 27 hereof and receives	**【Liabilities for causing severe damage to network security】** While not constituting a crime, it shall be subject to confiscation of illegal earnings and detention of less than 5 days by the public security authority and a fine ranging from 50,000 yuan to 500,000 yuan. Severe violation in this regard shall be subject to a detention of above 5 days but below 15 days and a fine ranging from 100,000 yuan to 1 million yuan. Any organization the conduct mentioned in the preceding paragraph shall be subject to confiscation of illegal earnings by the public security authority and a fine ranging from 100,000 yuan to 1 million yuan. The supervisor directly in charge and other directly liable persons shall

Related articles	Liabilities under the CSL	Liabilities under the Draft
	public security administrative punishment shall not be allowed to hold key posts of cybersecurity and network operation for 5 years, and any such person who receives criminal punishment shall not be allowed to hold key posts of cybersecurity and network operation for his/her lifetime.	be subject to penalty prescribed in the preceding paragraph. Any person who violates Article 27 hereof and receives public security administrative punishment shall not be allowed to hold key posts of cybersecurity and network operation for 5 years, and any such person who receives criminal punishment shall not be allowed to hold key posts of cybersecurity and network operation for his/her lifetime.
Article 46 Any individual or organization is responsible for his/its use of network, and shall neither establish any website or online communication group for the purpose of conducting fraud, transmitting criminal methods, making or selling prohibited or controlled items, or conducting other illegal criminal activities nor utilize the network to release information involving implementation of fraud, making or sales of prohibited or controlled items, and any other illegal criminal activity.	**【Liabilities for committing crimes through use of network】** If such violation does not constitute a crime, such individual or organization shall be subject to detention of less than 5 days by the public security authority and a fine ranging from 10,000 yuan to 100,000 yuan. Severe violation in this regard shall be subject to a detention of more than 5 days but less than 15 days and a concurrent fine ranging from 50,000 yuan to 500,000 yuan. The website or online communication group involved in the violation shall be closed. Those units with the conduct mentioned in the preceding paragraph shall be subject to a fine ranging from 100,000 yuan to 500,000 yuan by the public security authority. The supervisor directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph.	

Align with the PIPL on liabilities for violating personal information rights

Prior to the effective date of the PIPL (November 1, 2021), the competent authorities mainly imposed

administrative penalties for violations of personal information rights based on provisions in the CSL. Naturally, after the PIPL came into force, liabilities related to personal information protection in the CSL should be consistent with the PIPL to avoid any conflict in their application. The Draft would replace the penalty provisions in the current CSL on violating personal information rights with provisions that refer to the PIPL and other applicable laws and administrative regulations. On the one hand, the Draft retains the penalties that conform to related provisions of the PIPL. On the other hand, compared to the current CSL, the Draft would toughen legal liabilities for violations of personal information rights.

<table>
<tr><th>Related articles</th><th>Liabilities under the CSL</th><th>Liabilities under the Draft</th></tr>
<tr><td>Article 22 Paragraph 3 A provider of network products or services shall expressly notify and obtain consent of the users if the products or services collect user information; and if personal information of users are involved, the provider shall also comply with provisions of the present Law and the relevant laws and administrative regulations governing protection of personal information.</td><td rowspan="3">【Liabilities for violating personal information rights】
The competent authority shall order such operator or provider to make rectification and such operator or provider may be subject to one or combination of the following actions, depending on the severity of the circumstance: warning, confiscation of illegal earnings, a fine equivalent to more than 1 but less than 10 times the illegal earnings, or a fine less than 1million yuan and the supervisor directly in charge and other directly liable persons subject to a fine ranging from 10,000 yuan to 100,000 yuan if there is no illegal earnings. In case of severe violation, the competent authority may order suspension of related business, winding up for rectification, shutdown of website, and revocation of business license of such operator or provider.</td><td rowspan="3">【Liabilities for violating personal information rights】
Shall be subject to penalties pursuant to applicable laws and administrative regulations.</td></tr>
<tr><td>Article 41 Network operators shall abide by the “lawful, justifiable and necessary” principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected.
No network operator may collect any personal information that is not related to the services it provides. It shall collect and use, and process and store personal the information in the light of laws and administrative regulations and agreement with the users.</td></tr>
<tr><td>Article 42 No network operator may disclose, tamper with or destroy personal information that it has collected, or disclose such information to others without prior consent of the person whose personal information has been collected, unless</td></tr>
</table>

Related articles	Liabilities under the CSL	Liabilities under the Draft
such information has been processed to prevent specific person from being identified and such information from being restored. **A network operator shall take technical and other necessary measures to ensure the security of personal information it collects, and to protect such information from disclosure, damage or loss. In case of disclosure, damage or loss of, or possible disclosure, damage or loss of such information, the network operator shall take immediate remedies, notify the users in accordance with the relevant provisions, and report to competent authority.**		
Article 43 Each individual is entitled to require a network operator to delete his or her personal information if he or she founds that collection and use of such information by such operator violate the laws, administrative regulations or the agreement by and between such operator and him or her; and is entitled to require any network operator to make corrections if he or she founds errors in such information collected and stored by such operator. Such operator shall take measures to delete the information or correct the error.		
Article 44 No individual or organization may steal or otherwise unlawfully obtain any personal information, or sell or unlawfully provide any personal information to others.	**【Liabilities for violating personal information rights】** While not constituting a crime, it shall be subject to confiscation of illegal earnings by the public security authority and a concurrent fine equivalent to more than 1 but less than 10 times the illegal earnings or a	

Related articles	Liabilities under the CSL	Liabilities under the Draft
	fine less than 1 million yuan if there is no illegal earnings.	

Impose stricter legal liabilities for violating CII security protection obligations

For violations of national security review requirements for procurement by CII operators, the Draft would also raise the maximum fines to five percent of the violator's previous year's turnover. For violations of data localization and data export requirements for CII operators, the Draft refers to Article 46 of Data Security Law and Article 66 of the PIPL, both of which impose stricter legal liabilities on CII operators.

Related articles	Liabilities under the CSL	Liabilities under the Draft
Article 35 Any purchase of network products and services by the operator of critical information infrastructure that may threaten the national security is subject to the national security review conducted by the CAC together with competent departments of the State Council.	**【Liabilities for violating national security review requirement for CII procurement】** Shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than 1 but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine of ranging from 10,000 yuan to 100,000 yuan.	**【Liabilities for violating national security review requirement for CII procurement】** Shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than 1 but less than 10 times the purchase price or **not more than 5% of its turnover of the previous year**, and the supervisor directly in charge and other directly liable persons shall be subject to a fine of ranging from 10,000 yuan to 100,000 yuan.
Article 37 The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with	**【Liabilities for violating CII data storage and export requirement】** Shall be warned and ordered by the competent authority to make rectifications, and shall be subject to confiscation of illegal earnings and a fine ranging from 50,000 yuan to 500,000 yuan, and may be subject to suspension of related business, winding up	**【Liabilities for violating CII data storage and export requirement】** **Shall be subject to penalties pursuant to applicable laws and administrative regulations.**

Related articles	Liabilities under the CSL	Liabilities under the Draft
competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail.	for rectification, shutdown of website, and revocation of business license, and the supervisor directly in charge and other directly liable persons shall be subject to a fine ranging from 10,000 yuan to 100,000 yuan.	

Integrate liabilities for violating network information security obligations

The Draft integrates liabilities for violating network information security obligations, including user information governance, security management, and the establishment of network information security complaint and reporting systems. Similar to the aforementioned sections, the Draft raises the maximum fine to 50 million yuan or five percent of the violator's previous year's turnover and adds a prohibition on directly liable persons from taking management or key cybersecurity protection positions.

Related articles	Liabilities under the CSL	Liabilities under the Draft
Article 48 Paragraph 1 Electronic information sent and applications provided by any individual and organization shall be free of malwares and information that are prohibited by laws and administrative regulations from release or transmission.	**【Liabilities for providing malicious programs in the network】** The competent authority shall give a warning and an order of rectification. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.	**【Liabilities for violating information security management obligations】** The competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings. A fine up to 1 million yuan shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons. For any illegal act specified in the preceding paragraph with particularly serious
Article 47 A network operator shall strengthen the management of the information released by its users. If it founds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information, and take	**【Liabilities for violating information security management obligations】** The competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings. A fine of ranging from100, 000 yuan to	

Related articles	Liabilities under the CSL	Liabilities under the Draft
measures such as deletion to prevent dissemination of such information. The operator shall also keep relevant record, and report the case to the competent authority.	500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.	circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose a fine **ranging from 1 million to 50 million yuan or not more than 5% of its turnover of the previous year**, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine **ranging from 100,000 yuan to 1 million yuan** shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to **prohibit the said persons from acting as directors, supervisors, senior executives or holding key posts of cybersecurity and network operation.**
Article 48 Paragraph 2 Providers of electronic information transmission service and application download service shall assume the obligations of security management. If any such provider becomes aware that its user engages in any act mentioned in the preceding paragraph, such provider shall immediately stop providing such service, take measures such as deletion, keep the record, and report to competent authority.		
Article 49 A network operator shall establish network information security complaint and reporting mechanisms, and shall release the complaint and reporting channels to promptly accept and settle complaints and reports concerning network information security. **Network operators shall cooperate with the Cyberspace administration and any other competent authority in their lawful inspections and supervisions.**	**【Liabilities for hindering enforcement of competent authorities】** Shall be warned and ordered by the competent authority to make rectifications. A fine of ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.	
Article 12 Paragraph 2 Individuals and organizations using the network shall comply with the Constitution and laws, follow the public order, and show respect for social moralities, and shall neither impair cybersecurity nor engage	**【Liabilities for release or transmission of prohibited information】** Shall be subject to penalties pursuant to applicable laws and administrative regulations.	**【Liabilities for release or transmission of prohibited information】** Shall be subject to penalties pursuant to applicable laws and administrative regulations. Where there are no provisions

Related articles	Liabilities under the CSL	Liabilities under the Draft
in activities, by making use of the network, that endanger national security, honor and interests, incite subversion of the state power or overthrow of the socialist system, incite splitting of the country, undermine national unity, advocate terrorism and extremism, ethnic hatred and discrimination, spread violent and pornographic information, fabricate and disseminate false information to disrupt economic and social orders, or infringe upon the reputation, privacy, intellectual property and other legitimate rights and interests of others.		on such cases, the competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings. A fine **up to 1 million yuan** shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons. For any illegal act specified in the preceding paragraph with particularly serious circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose a fine **ranging from 1 million to 50 million yuan or not more than 5% of its turnover of the previous year**, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine **ranging from 100,000 yuan to 1 million yuan** shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to **prohibit the said persons from acting as directors, supervisors, senior**

Related articles	Liabilities under the CSL	Liabilities under the Draft
		executives or holding key posts of cybersecurity and network operation.

Conclusion

The Draft mainly focuses on imposing stricter liabilities for violations of the CSL and conforming to the PIPL on the maximum penalties of both the company and persons directly liable, thereby reflecting China's strong attitude toward cybersecurity protection. The Draft is currently open for public comments and there remains significant time before it may enter into force. Therefore, parties who engage in network operations should continue to actively fulfill their obligations relating to network operation security, network information security, and personal information protection, and monitor this and other legislative developments.

2. CAC Issues Guidelines for Data Export Security Assessment

Authors: Kevin DUAN | Kemeng CAI | Zihuan XU | Ziqian ZHANG

On August 31, 2022, the Cyberspace Administration of China (the "**CAC**") issued the *Application Guidelines for Security Assessment of Cross-border Data Transfer (1st Edition)* (the **"Application Guidelines"**), which specify and implement the provisions on cross-border data transfer security assessments ("**security assessments**") in the *Measures for Security Assessment of Cross-border Data Transfers* (the "**Assessment Measures**"). The Application Guidelines clarify the application scope of security assessments, stipulate the means, procedures and required materials for the application, and provides contact information for inquiries regarding the application. The Application Guidelines also contain template documents, including the Cross-border Data Transfer Security Assessment Application Letter (the "**Application Letter**") and the Cross-border Data Transfer Risk Self-Assessment Report Template (the "**Self-Assessment Report Template**"), which offer effective guidance and assistance to data handlers who seek a security assessment.

This article briefly analyzes the new requirements set out in the Application Guidelines and highlights critical issues throughout the security assessment application while building on the key points of the Assessment Measures explained in our July 19 article, *CAC Formally Promulgates the Assessment Measures for Data Export.*

Reaffirming the scope of security assessments

The Application Guidelines reaffirm the circumstances subject to mandatory security assessments in accordance with Article 4 of the Assessment Measures[1], and further clarify the criteria for determining cross-border data transfer activities, which is:

- Data handlers who transfer and store data collected and generated in the course of operations in Chinese Mainland to overseas;
- Data handlers who store data collected and generated in Chinese Mainland, but provide overseas institutions, organizations, and individuals with right of access, retrieve, download and export;
- Other cross-border data transfer activities prescribed by the CAC.

Compared to the CAC's introduction in a press briefing on July 7, 2022[2], in which the second circumstance was described as "provide overseas institutions, organizations, and individuals with the right to access and

[1] Article 4 of the Assessment Measures: "Where a data handler transfers data abroad under any of the following circumstances, it shall, through the local Cyberspace Administration at the provincial level, apply to the State Cyberspace Administration for security assessment for the outbound data transfer: (1) a data handler who transfers Important Data abroad; (2) a critical information infrastructure operator, or a data handler processing the personal information of more than 1 million individuals, who, in either case, transfers personal information abroad; (3) a data handler who has, since January 1 of the previous year cumulatively transferred abroad the personal information of more than 100,000 individuals, or the sensitive personal information of more than 10,000 individuals, or (4) other circumstances where the security assessment for the outbound data transfer is required by the State Cyberspace Administration."

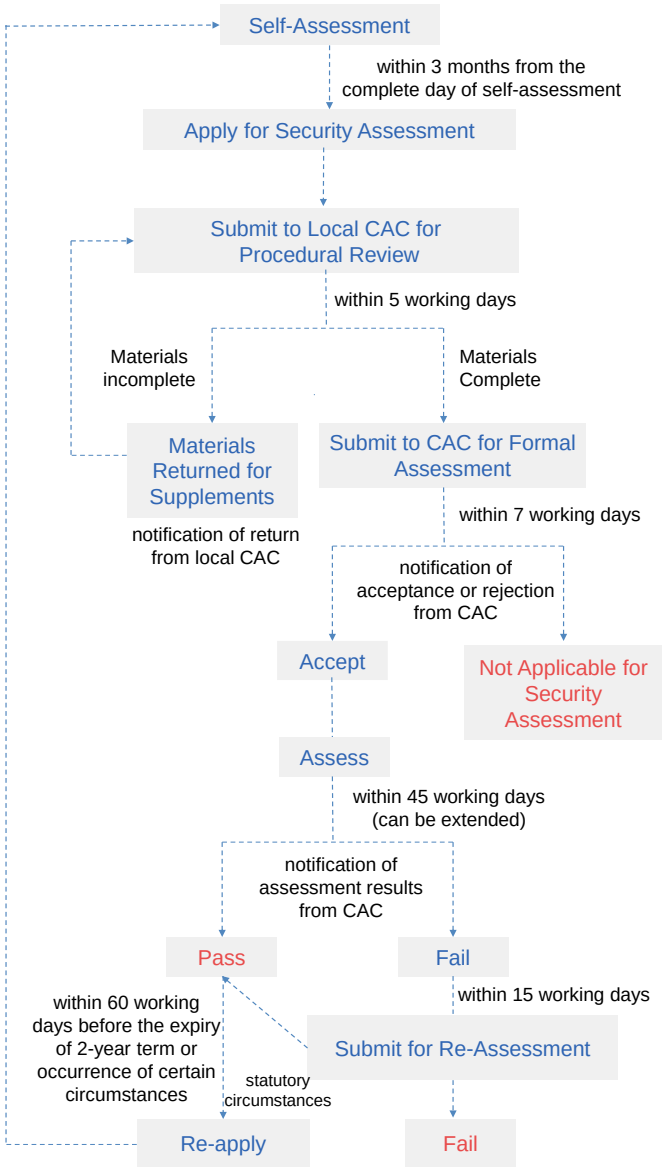
[2] CAC's press briefing on the Assessment Measures, published on July 7, 2022; for more details, please refer to: http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm (last accessed on September 7, 2022).

use such data", the Application Guidelines further specify remote access as "providing overseas institutions, organizations, and individuals with the right of access, retrieve, download, and export".

Notably, the Application Guidelines add a miscellaneous provision to cover "other cross-border data transfer activities prescribed by the CAC", which leaves room for future interpretations when the regulatory authorities deal with complicated data export situations. However, the Application Guidelines do not directly address the direct collection of data from overseas, i.e., where overseas entities directly collect personal information from personal information subjects residing in Chinese Mainland. Therefore, it is advisable for relevant enterprises to closely monitor regulatory developments in this regard and to take corresponding compliance measures when appropriate.

Specifying the application method and procedures

On the basis of Article 7 and Articles 11-13 of the Assessment Measures, the Application Guidelines detail the method and procedures for applying for security assessments with the CAC. The basic process is illustrated by the following diagram:



Key points of the aforementioned procedures are as follows:

I. Self-assessments must be completed within three months of the date of application

According to the templates provided as annexes to the Application Guidelines, the Letter of Commitment and the Self-Assessment Report Template both require that a cross-border data transfer risk self-assessment ("**self-assessment**") be completed within three months of the date of application, and no significant changes have occurred on or before the date of application.

II. Applications to be submitted on-site

According to Application Guidelines, data handlers will submit application materials to the provincial-level CAC in written form and also attach a digital version. A digital version of materials is to be submitted via a compact disc.

III. Three types of notifications may be sent during the application process

On the basis of the Assessment Measures, the Application Guidelines provide three notifications that data handlers may receive at three important stages during the application process. These notifications are as follows:

- When data handlers fail to pass the completeness check, the CAC at the provincial level will send a notification to return the materials and to request supplements.
- When the formal assessment is completed, the CAC will send a written notification to inform the data handlers whether their application is accepted.
- When the security assessment is completed, the CAC will send data handlers notification of the assessment results. If there is no objection to the results, the data handlers will regulate their cross-border data transfer activities in accordance with the relevant laws and regulations and requirements stipulated in the notification. In case of any objection, data handlers have a 15-day period to submit for a re-assessment, starting from the date of receipt of the notification of the assessment results, according to Article 13 of the Assessment Measures.

Regarding the official assessment period, Article 12 of the Assessment Measures provides a 45-working-day period, while permitting an extension in the case of complicated situations or material supplements and corrections. However, an abundance of applications may be expected in the short term, given the generally low thresholds for mandatory security assessments as stipulated in the Assessment Measures and the short six-month cure period. Hence, it is possible that the regulatory authorities will not conduct a substantive review in certain cases and permit data exports within a relatively short time for applications that are from less sensitive industries, present a high level of need to engage in cross-border transfer activities, and contain less sensitive outbound data.

IV. Application inquiries may be made

To provide the enterprises a channel to seek official instructions in case of practical problems, the Application Guidelines contain contact information for inquiries related to the security assessment as follows:

- E-mail address: sjcj@cac.gov.cn
- Tel: 010-55627135

As of the date of this newsletter, the Beijing Cyber Administration has set up a hotline for inquiries regarding the security assessment application (010-67676912) and some other provincial-level CACs release their own contact information accordingly. It is advisable for enterprises to take notice of the relevant information disclosed by the regulatory authorities.

Specifying the requirements of the application materials

Compared with Article 6 of the Assessment Measures, the Application Guidelines further specify the application materials that data handlers should submit when applying for a security assessment and provide corresponding templates, including:

- Photocopy of unified social credit code certificate;
- Photocopy of ID card of the legal representative;
- Photocopy of ID card of the case handler;
- Power of attorney for the case handler;
- Application letter for Security Assessment, including the letter of commitment and the Application Form;
- Photocopies of cross-border transfer related contracts or other legally binding documents to be concluded with the overseas receivers;
- Self-Assessment report on cross-border data transfer risks;
- Other relevant supporting materials.

Key points of the aforementioned materials are as follows:

I. Security assessment "case handler" is introduced for the first time

The Application Guidelines introduces the role of "case handler" for the first time. According to the power attorney for the case handler and the Application Letter of the Security Assessment in the appendix, the case handler shall be the authorized employee of the data handler and in charge of the application work on behalf of the data handler, including filing in the Application Letter of the Security Assessment.

II. Both the data transferor and the data receiver should appoint personnel and a management department responsible for data security

Pursuant to the Application Letter annexed to the Application Guidelines, data handlers need to provide information regarding their personnel and management department responsible for data security and those of their overseas receivers.

This data security personnel and management department requirement is imposed on data handlers who process important data or personal information, and who are critical information infrastructure operators, by Article 27 of *Data Security Law*, Article 52 of *Personal Information Protection Law,* and Article 14 of *Regulation on Protecting the Security of Critical Information Infrastructure*. In addition, *Information security technology-Personal Information Security Specification (GB/T35273-2020)* [3] further specifies the criteria for determining whether a person and a department responsible for personal information protection are needed. Building on these laws and regulations, the Application Guidelines require data handlers to fill in the information of data security personnel and management department. However, this may raise the question what information data handlers should provide if they are not required to designate data security personnel and management department under the aforesaid laws, regulations and standard, and we consider such handlers may provide the information of the IT responsible personnel instead.

In addition, it should be highlighted that information should be submitted regarding the personnel and management department of the overseas data receiver. Therefore, enterprises who may be involved in applying for security assessments due to use of overseas data processing services are advised to take into account the conditions of responsible personnel and organization when selecting their service providers. Enterprises should also consider including relevant clauses to guarantee that providers appoint the personnel and department as required, so as to fulfil the requirements of the security assessment.

III. Applications can be made for exports of important data and personal information at the same time

In column "09 Information of Proposed Cross-border Data" in the annexed Application Form, applicants

[3] Article 27 of Data Security Law: "The carrying out of data handling activities shall be in accordance with laws and regulations, establishing and completing data security management systems for the entire process, organizing and carrying out education and training on data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The carrying out of data handling activities through information networks, i.e., the Internet, shall fulfill the duties to protect data security on the basis of the multi-level protection system for cybersecurity.

Those processing important data shall clearly designate persons responsible for data security and data security management bodies to implement responsibilities for data security protection."

Article 52 of the PIPL: "A personal information processor that processes the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity shall appoint a person in charge of personal information protection to be responsible for overseeing personal information processing activities as well as the protection measures taken, among others.

The personal information processor shall disclose the contact information of the person in charge of personal information protection, and submit the name and contact information of the person in charge of personal information protection to the authority performing personal information protection functions."

Article 14 of the Regulation on Protecting the Security of Critical Information Infrastructure: "The operator shall set up a special security management organization, and conduct security background examination on the person in charge of the special security management organization and the personnel in key positions. During the review, the public security organ and the state security organ shall provide assistance."

Information security technology personal information security specification (GB/T 35273-2020) 11.1: "Organizations meeting one of the following conditions shall set up full-time personal information protection director and personal information protection work organization to be responsible for personal information security: (1) the main business involves personal information processing, and the number of employees is more than 200; (2) the organization meets one of the following conditions: Processing personal information of more than 1 million people, or expected to process personal information of more than 1 million people within 12 months;(3) Processing sensitive personal information of more than 100,000 people. "

are allowed to fill in the cross-border transfer information of both important data and personal information at the same time. Also, the "Information of Proposed Cross-border Data" section in the Application Letter no longer requires their distinction. This implies that personal information and important data transferred to the same overseas receiver can be the subject of the same application for security assessment. However, it remains unclear whether this is applicable in cases where data is provided to multiple overseas receivers within the corporate group under the same export circumstances, which is an issue facing many multinationals. The Application Guidelines have left this issue for future clarification as the regulations are implemented in practice.

IV. "Legal Documents" defined

Article 8 of the Assessment Measures[4] lists "the legal documents to be concluded between the data handler and the overseas receiver" as one of the key contents of the security assessment, but does not define the "legal documents" concept. The Application Guidelines clearly interpret the concept as "cross-border data transfer-related contracts or other legally binding documents".

Pursuant to the Application Guidelines, to complete the application form, data handlers need to provide the clauses in accordance with the necessary contents one by one as required by Article 9 of Assessment Measures[5].

In view of the strict legal document requirements for a security assessment, it is advisable that enterprises refer to or use the standard contractual clauses of cross-border transfer of personal information issued by the CAC, or ensure that relevant provisions are introduced strictly as prescribed in the Assessment Measures in other legal documents (such as the unilateral letters of commitment from the overseas receiver, or the data security management system or policy of the groups of the parties in Chinese Mainlandor overseas).

In addition, the Application Guidelines clearly state that the Chinese version of legal documents shall prevail. In the case where only a non-Chinese version is available, an accurate Chinese translation is required to be submitted alongside.

---

[4] Article 8 of the Assessment Measures: "Prior to applying for the security assessment for the outbound data transfer, a data handler shall, in advance, conduct a self-assessment on the risks of the outbound data transfer, and the self-assessment shall focus on the following matters:…(5) whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts for the outbound data transfer, or other legally binding documents to be concluded with the foreign receiver…"

[5] Article 9 of Assessment Measures: "A data handler shall expressly agree on the responsibilities and obligations for data security protection in the Legal Documents concluded with the foreign receiver, which shall, at least, include the following matters: (1) the purpose, method and scope of the data to be transferred abroad, and the purpose and method for processing the data by the foreign receiver; (2) the location and duration for the storage of the data located abroad, as well as how to process the data located abroad upon the expiry of the storage period, achievement of the agreed purpose, or termination of the Legal Documents; (3) restrictions on the foreign receiver's re-transfer of the data located abroad to another organization or individual; (4) security measures which should be taken in case of a material change to the actual control or business scope of the foreign receiver, or in case of a change to the data security protection policies or regulations, or network security environment of the country or region where the foreign receiver is located, or in case that the data security cannot be guaranteed as a result of any other force majeure event; (5) remedial measures, liability for breach of contract and dispute resolution mechanism in the event of a violation of data security protection obligations as agreed in the Legal Documents; and (6) requirements on properly responding to a data security incident, as well as channels and method to safeguard individuals' personal information rights, when the data located abroad is tampered with, destroyed, leaked, lost, transferred, illegally obtained or illegally used."

V. Compliance with Chinese laws and regulations is highlighted

The Application Guidelines require data handler to submit in its application form its "compliance with Chinese laws, administrative regulations and department regulations". In particular, the data handler is required to briefly describe the administrative penalties and the investigation and rectification by the relevant competent regulatory authorities in its business operations over the past two years, focusing on data security and cybersecurity.

Providing the Self-Assessment Report Template

According to Article 5 of the Assessment Measures[6], data handlers must conduct a cross-border data transfer risk self-assessment ("**self-assessment**") prior to submitting an application for security assessment. Furthermore, Article 6 requires the data handlers to submit the cross-border data transfer risk self-assessment report to the competent authorities, which means that the self-assessment report is a significant subject of the security assessment process. Annex 4 to the Application Guidelines contains the Self-Assessment Report Template, in which the factual materials to be submitted and evaluation criteria are to be addressed are clarified through instructions.

I. Submission of the Self-Assessment Report

When applying for a security assessment to the CAC at the provincial level, the data handler shall submit a complete and authentic Self-Assessment Report alongside. It should be noted that if a third-party organization involves in the Self-Assessment, its basic information and involvement shall be stated in the Self-Assessment Report. Meanwhile, official seals of the third-party organization on relevant pages are mandatory. Analyzing from the overall requirements of the Application Guidelines, "basic information of the third party organization" may include the name, nature of entity, main business situation, registered address and business address, while "participation" may refer to the work and role of the third party in the Self-Assessment.

II. Coverage and new requirements in the Self-Assessment Report Template

The Self-Assessment Report Template is divided into four parts: a brief introduction of self-assessment work, the overview of cross-border data transfer activities, the risk assessment of proposed cross-border data transfer activities, and a conclusion of the risk assessment.

The first part of the Self-Assessment Report Template mainly summarizes the self-assessment work,

[6] Article 5 of the Assessment Measures: "Prior to applying for the security assessment for the outbound data transfer, a data handler shall, in advance, conduct a self-assessment on the risks of the outbound data transfer, and the self-assessment shall focus on the following matters: (1) the legality, legitimacy and necessity of the purpose, scope and methods of the outbound data transfer, and the processing of the data by the foreign receiver; (2) the scale, scope, type and sensitivity of the outbound data transfer, and the risks to national security, the public interest or to the legitimate rights and interests of individuals or organizations, caused by the outbound data transfer; (3) the duties and obligations which the foreign receiver commits to perform, and whether the foreign receiver's organizational and technical measures and capabilities in terms of performing the duties and obligations can guarantee the security of the outbound data transfer; (4) the risks of the data being tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the outbound data transfer, and whether there is a smooth channel for safeguarding personal information rights and interests; (5) whether the responsibilities and obligations for data security protection are fully agreed in relevant contracts for the outbound data transfer, or other legally binding documents to be concluded with the foreign receiver; and (6) other matters that may affect the security of the outbound data transfer."

including the start and end time, organization, implementation process, and methods, etc. We believe third-party involvement may be disclosed in this section. The second part is intended to cover the business of the data handler and the facts of the cross-border data transfers, including the basic information of the data handler, the design of the transfer business, the conditions of the information systems, the overview of proposed cross-border data transfer, the security assurance capabilities of the data handler, the information of the overseas data receiver, data security protection obligations and responsibilities agreed in the legal documents, and other circumstances the data handler considers necessary to describe. Among them, the "data security protection obligations and responsibilities agreed in the legal documents" are in line with Article 9 of the Assessment Measures concerning the data security protection responsibilities and obligations. It should be stressed that the second part of the self-assessment report has extended the coverage of the material facts related to cross-border data transfers. The added items are as follows:

- In addition to the facts involved in the cross-border data transfer activities, other basic information of the data handler, other than the enterprise information open to the public, are to be submitted, including basic information of organization or individual, information of equity structure and actual controller, information of organization structure, information of data security management department, overall information of business and data, information of domestic and overseas investment;
- The basic information of the facilities that may be involved in the cross-border data transfer activities shall be introduced comprehensively, including information of data assets related to the business of cross-border data transfers, information of information system in Chinese Mainland and overseas, information of data centers (including cloud services) related to cross-border data transfers, information of cross-border data transfer links (such as the provider, number and bandwidth of the links);
- It is necessary to disclose information about providing cross-border data to other overseas receivers through onward transfers after the cross-border data transfer;
- In terms of the security assurance capabilities of the data handler, the self-assessment report builds on the *Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)* and further requires the data handler to illustrate its internal categorization and classification of data, the development of its risk assessment system, as well as its compliance with laws and regulations pertaining to data and cyber security;
- As regards to the overseas receiver, the self-assessment report adds that it shall include a "description of the whole process of data processing by the overseas receiver", which covers the data life cycle from the collection by the overseas receiver from Chinese Mainland, to the use, retention, disclosure and deletion.

The third part of the Self-Assessment Report Template basically restates the requirements of the cross-border data transfer risk assessment in Article 5 of the Assessment Measures, which instructs data handlers to conduct risk assessment based on the facts specified in the second part. Meanwhile, the Self-Assessment Report Template adds a requirement to explain the risk assessment and focus on

the problems and potential risks found in the assessment, as well as the corresponding rectification measures and rectification effects. Thus, in addition to the risk assessment of the proposed cross-border data transfer, the data processor also needs to disclose the rectification measures taken to mitigate the risk and the outcomes therefrom.

Our comments

As the Assessment Measures take effect, enterprise cross-border data transfers are entering a phase of compliance rectification, for which the Application Guidelines offer detailed instructions and a roadmap. Pursuant to the Assessment Measures and the Application Guidelines, it is advisable for enterprises to mitigate compliance risks for their data exports by addressing the following:

- Specify the circumstances of cross-border data transfers throughout data processing activities and examine the relevant facts. Determine whether these circumstances fall within the scope of the security assessment and select a data export strategy accordingly (such as to pursue complete data localization or apply for a security assessment as prescribed by laws and regulations);
- Refer to the second part of the Self-Assessment Report Template to conduct a self-assessment in a timely manner. Identify the potential risks and take corresponding mitigation measures so as to pass the security assessment within the six-month period provided in the Assessment Measures;
- Prepare the application materials as required by the Application Guidelines and submit to the relevant CAC at the provincial level, including the photocopy of unified social credit code certificate, photocopy of ID card of the legal representative, photocopy of ID card of the case handler, power of attorney for the case handler, the Application Letter for Security Assessment, including the letter of commitment and the Application Form, photocopies of cross-border transfer related contracts or other legally binding documents to be concluded with the overseas receivers, a self-assessment report, etc.;
- Establish an internal compliance system for cross-border data transfer security assessments. Continue to monitor the conditions of all data exports. Update the submitted materials and re-apply for a security assessment when required.

Important Announcement

This Newsletter has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Beijing	**Wenyu JIN**	**Attorney-at-law**
	Tel:	+86 10 8525 5557
	Email:	wenyu.jin@hankunlaw.com
Shanghai	**Yinshi CAO**	**Attorney-at-law**
	Tel:	+86 21 6080 0980
	Email:	yinshi.cao@hankunlaw.com
Shenzhen	**Jason WANG**	**Attorney-at-law**
	Tel:	+86 755 3680 6518
	Email:	jason.wang@hankunlaw.com
Haikou	**Jun ZHU**	**Attorney-at-law**
	Tel:	+86 898 3665 5000
	Email:	jun.zhu@hankunlaw.com
Wuhan	**Jiao MA**	**Attorney-at-law**
	Tel:	+86 27 5937 6200
	Email:	jiao.ma@hankunlaw.com
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com