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

Han Kun Newsletter

Issue 171 (7th edition of 2021)

Legal Updates

1. Analysis of Revised Draft Cybersecurity Review Measures
2. Brief Review of Provisions on Administration of Security Vulnerabilities in Network Products

1. Analysis of Revised Draft Cybersecurity Review Measures

Authors: Kevin DUAN | Tracy ZHOU | Charles WU | Kemeng CAI

On 10 July 2021, the Office of the Central Cyberspace Affairs Commission and the Office of Cybersecurity Review under the Cyberspace Administration of China ("**CAC**") promulgated the Measures for Cybersecurity Review (the "**Review Measures**") (Revised Draft for Comments) (the "**Draft**"). The Draft extends the scope of cybersecurity reviews to data processors ("**Processors**") engaging in data processing activities that affects or may affect national security, including listing in a foreign country. This article is a preliminary interpretation of the Draft, and analyses its potential impact.

Overview of the Draft

I Expansion of the scope of review to include specific data processors who list in a foreign country

Based on the Cybersecurity Law and the Review Measures, the target subjects of the cybersecurity review system are critical information infrastructure operators ("**CIIO**") who purchase Network Products and Services, as set out by Article 2 of the Review Measures[1]. In addition, the relevant regulatory authorities are also entitled to impose security reviews on Network Products and Services that are deemed capable of affecting national security, as set out in Article 15 of the Review Measures, without the need for the operator to be a CIIO. Building on the foundation of the Review Measures, Article 2 of the Draft clearly sets forth that data processors ("**Operators**") who engage in data processing activities, which affects or may affect national security, are included in the scope of cybersecurity review.

II Operators with more than 1 million users' personal information data, which are listing in a "foreign country", are obliged to apply for a mandatory cybersecurity review

The Draft states that "**Operators listing in a foreign country with more than 1 million users' personal information data must apply for a cybersecurity review with the Cybersecurity Review Office**." Therefore, non-CIIOs are still obliged to file for a cybersecurity review prior to a non-PRC listing if they process data exceeding this threshold. To better facilitate the review, the Draft adds the CSRC to the review bodies, which is led by CAC and joined by twelve other authorities. This provision on the number of users contains ambiguities, such as whether the term "1 million users" refers to PRC users only or includes non-PRC users.

[1] "Network Products and Services" mainly refer to core network equipment, high-performance computers and servers, large-capacity storage equipment, large databases and application software, network security equipment, cloud computing services, and other Network Products and Services that may substantially impact Critical Information Infrastructure.

III Review focus and the expansion of review standards from cybersecurity to data security

In the past, the Review Measures mainly focused on supply chain security risks associated with CIIOs purchasing specific Network Products and Services. The Draft expands this scope by confirming that its legislative basis is the Data Security Law, which is apart from the Cybersecurity Law and will take effect on 1 September 2021. Namely, the scope of review now extends to CIIOs, Processors carrying out data processing activities, and national security risks related to a non-PRC listing, especially "*risks of core data, important data or substantial personal information being stolen, leaked, damaged, illegally used or exported; risks of Critical Information Infrastructure, core data, important data or substantial personal information data being affected, controlled and maliciously used by foreign governments after a foreign listing.*" It should be noted that "core data"[2] and "important data"[3] are important concepts in the Data Security Law. The scope of these concepts is yet to be determined.

IV Changes to application materials and the review process

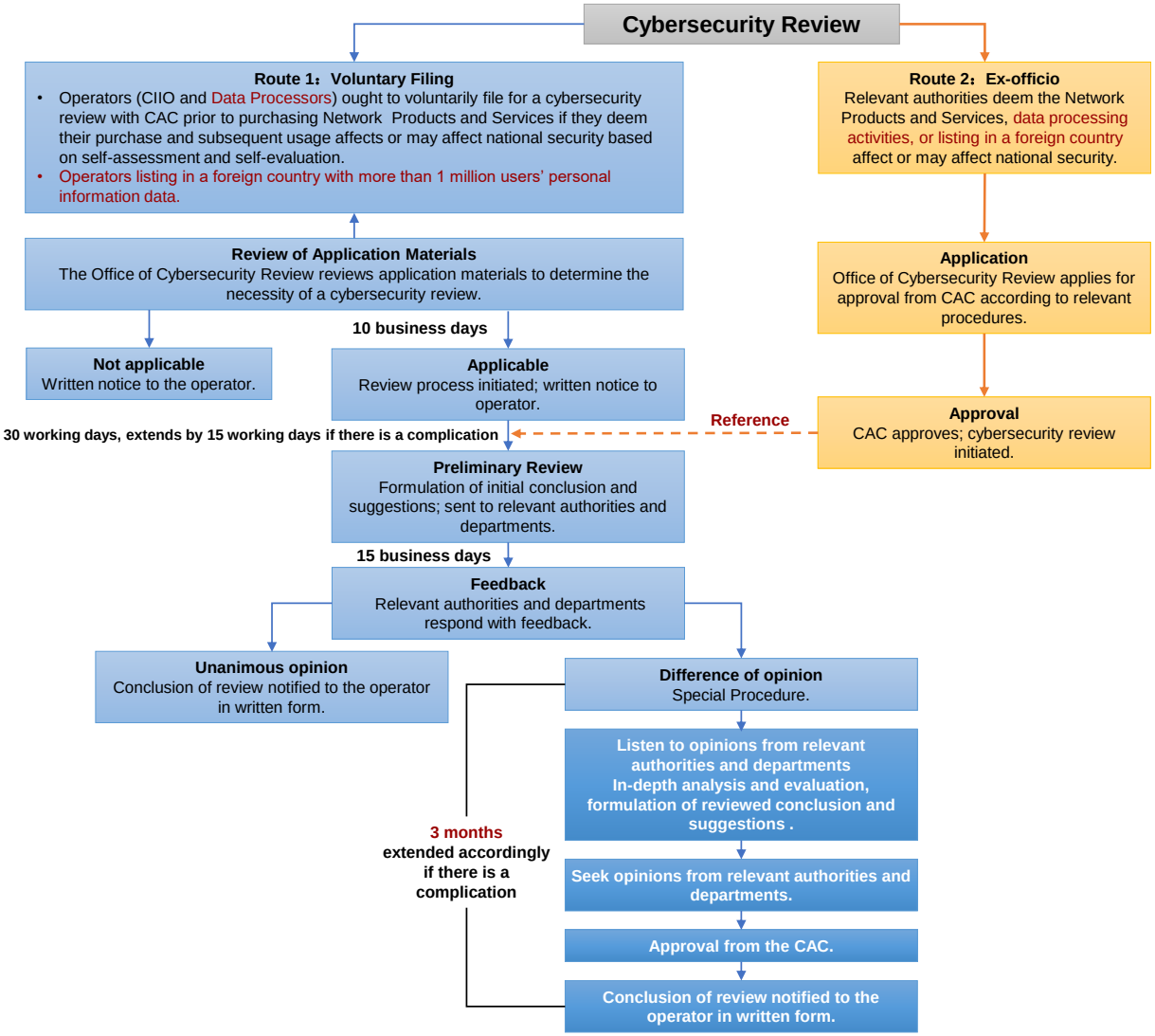
Taken as a whole, the application materials and the review process set forth in the Review Measures have stayed relative intact. However, companies listing in a foreign country need to submit "proposed IPO materials" for review. Considering the quantity of materials that needs to be submitted for a non-PRC IPO, the specific scope and focus of review requires clarification in practice.

According to a response to a journalist's question when the Review Measures were issued, cybersecurity reviews are delegated to the China Cybersecurity Review Technology and Certification Center (the "**CCRTC**"), who is responsible for tasks including the admission of materials, preliminary review of materials, and organisation of each specific review under the leadership of the Cybersecurity Review Office.

The review process set forth in the Draft follows that of the Review Measures, but adds that in case there is disagreement between the members of the cybersecurity review group and the relevant Critical Information Infrastructure protection departments, there will be a special review process seeking the opinions of relevant authorities and the case will be reported to CAC. In this case, the review period is extended from 45 business days to 3 months, subject to further extensions should complications arise. The overall review process according to the Draft is shown in the figure below. If adopted in their current form, this means that in practice, transaction parties in a foreign IPO should be prepared to wait potentially 5-6 months, to allow for a cybersecurity review to be completed.

[2] Article 21 of the Data Security Law states that "*data that have a bearing on national security, the lifelines of national economy, people's key livelihood and major public interests shall constitute the core data of the State and shall be subject to stricter management system*."

[3] Article 21 of the Data Security Law states that "*the national data security coordination mechanism shall make overall planning for and coordinate relevant departments in formulating the catalogues for important data and strengthening the protection of important data… Each region and department shall, in accordance with the classified and graded data protection system, determine the specific catalogue for important data for the respective region and department, and in relevant industries and areas, and undertake special protection for the data included in the catalogue*".



The impact on China concepts companies listing in a "foreign country"

I Whether "listing in a foreign country" includes listing in Hong Kong

We note that the Draft uses the concept of "listing in a foreign country" [typically understood to mean outside of China, including Hong Kong], which deviates from concepts used in prior laws and regulations, such as the Securities Law and its subordinate policies and in data security policies, which used the "domestic" and "abroad" / "overseas" [typically understood to mean the jurisdiction of Chinese mainland and a jurisdiction outside of Chinese mainland.]. For example, Article 2 of the Securities Law state that "*[t]he Law is applied to the issuance and trading of stocks, corporate bonds, depository receipts and other securities lawfully recognized by the State Council within the territory of the People's Republic of China*"; Article 224 states that "[*any] domestic enterprise that seeks to issue securities abroad either directly or indirectly or that lists its securities to be traded abroad shall comply with the relevant provisions of the State Council*." Article 37 of the Cybersecurity Law states that "[*CIIO] shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted*

in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail." Therefore, given this context, the linguistic choice of "listing in a foreign country" as opposed to the more commonly used phrases in securities regulations "abroad" / "overseas", appears to be intentional. This suggests that the scope of the cybersecurity review does not extend to companies listing in Hong Kong. However, as the Draft lacks explicit explanation, the verdict is still out on the scope of the term and is subject to the finalization of the Review Measures by relevant authorities or clarifications in practice.

II Whether "listing in a foreign country" includes SPACs, RTOs, Directing Listings etc.

Apart from IPOs, CCS companies may list in the US via SPACs (Special Purpose Acquisition Companies), RTO (Reverse Takeovers), direct listings etc. Although the Draft only requires the disclosure of "proposed IPO materials", in light of the fact that CCS companies will need to publicly disclose or provide information to foreign exchanges during the listing process, regularly disclose information after listing, and remain subject to investigation and supervision by foreign exchanges and securities regulatory authorities, these other methods of listing may also give rise to the same cybersecurity risks. Namely, these risks are national security risks associated with listing in foreign countries as mentioned in the Draft, including "*risks of core data, important data or substantial personal information being stolen, leaked, damaged, illegally used or exported; risks of Critical Information Infrastructure, core data, important data or substantial personal information data being affected, controlled and maliciously used by foreign governments after foreign listing*." In our view, regardless of the method of listing, listing in the US or other foreign countries may give rise to PRC cybersecurity review.

III Whether "listing in a foreign country" includes a secondary listing in Hong Kong

If "listing in a foreign country" excludes listing in Hong Kong as interpreted in Section (1), then we take the view that a secondary listing in Hong Kong should not give rise to cybersecurity reviews either.

However, if the finalized Review Measures confirm that cybersecurity reviews will apply to companies listing in Hong Kong, then we take the view that the scope of review will extend to secondary listings in Hong Kong. This is because during and after a secondary listing in Hong Kong, CCS companies may need to disclose or provide additional information in accordance with the Listing Rules of Hong Kong, and will be subject to supervision and investigation by the Stock Exchange of Hong Kong and securities regulatory authorities. Therefore, for CCS companies that have passed a cybersecurity review or listed prior to the implementation of the Review Measures, a secondary listing in Hong Kong present additional data security risk.

IV Impact on follow-on offerings and bond offerings of CCS companies listed in foreign country

The Draft does not specify whether follow-on offerings and bond offerings of CCS companies already listed in foreign country are subject to cybersecurity reviews. We are inclined to believe that follow-on offerings and bond offerings, especially of companies that have already passed cybersecurity reviews during their listing, may be outside the scope of review. First, the Draft states that "***Operators***

listing in a foreign country with more than 1 million users' personal information data" are subject to cybersecurity review, not issuing or listing securities. Second, for CCS companies already listed in foreign countries, follow-on offerings and bond offerings will not impact the information disclosure rules to which they are subject, and supervision and investigation by foreign exchanges and securities regulatory authorities. Therefore, in this respect, the data security risk will not materially increase. However, as the CCS companies may disclose additional financial information apart from what is disclosed in regularly disclosed annual or quarterly reports for follow-on offerings and bond offerings, additional data security risks cannot be eliminated. Therefore, the verdict on (ii) the application of the cybersecurity review on follow-on offerings and bond offerings of CCS companies, (ii) whether CCS companies that have passed cybersecurity reviews during listing still need to complete cybersecurity reviews for follow-on offerings and bond offerings and (iii) whether the cybersecurity reviews apply to CCS companies that have not completed cybersecurity reviews (including those listed prior to the implementation of the Review Measures, or those not meeting the standard of review at the time of listing), is still unclear, and subject to the finalized Review Measures by the relevant authorities or clarification in practice.

V Whether the Draft operates retrospectively on CCS companies already listed in foreign countries

The Draft does not explicitly require CCS companies that have already listed in foreign countries prior to the implementation of the Review Measures to apply for cybersecurity reviews. However, Article 16 of the Draft states that: "*the Network Products and Services, data processing activities and listings in foreign countries deemed to affect or may affect national security by members of the cybersecurity review group are subject to review in accordance with this Measures, after approval is obtained from the CAC by the Cybersecurity Review Office.*" Under this provision, the regulatory authorities are entitled to conduct security reviews on foreign-listed CCS companies in respect of their day-to-day data processing activities. During such a review, the authorities may take into account the fact that the company is listed in a foreign country.

Not passing cybersecurity reviews imposed on listings (and follow-on offerings and bond offerings) of CCS companies has clear consequences, namely the listing, follow-on offering and bond offering of the company will be restricted. However, if the cybersecurity review does not pass with respect to an already listed CCS company, the consequences are yet to be clarified by laws and regulations.

Recommendations

For companies processing substantial personal information or sensitive data, especially those that plan on listing outside of Chinese mainland, to maximize their chances of passing the cybersecurity review, we recommend:

- Stay up-to-date on the personal information protection policies of regulatory authorities; avoid collecting personal information irrelevant to services, especially sensitive personal information; continuously improve user information protection.

- Closely follow subsequent identification standards for “important data” released by regulatory authorities; implement requirements, such as important data protection, security risk assessment, data localization, etc. comprehensively; establish a data security impact assessment system and an internal compliance governance system to carry out prior assessment of high-risk data processing activities and continuous data compliance audits.
- Further refine the supply chain security review of Network Products and Services by (i) advanced assessment of supplier compliance; (ii) imposition of undertakings in agreements; (iii) auditing during and after cooperation, to mitigate the risk that the Network Products and Services cause the Operator’s system to be illegally controlled or interfered, or its data disclosed, stolen or damaged. Also, to ensure that the supply chain is safe, open, transparent, diverse and sustainable, and will not be subject to illegal control or interference, and can effectively prevent data leakage, theft or damage.
- Prior to submitting data and information to foreign exchanges and regulatory authorities, seek the prior consent from CAC, the CRSC and other relevant authorities in accordance with Section 36 of the Data Security Law, Section 17 of the Securities Law and other laws and regulations. Formulate an internal system explicitly confirming the preceding requirement.
- Pay close attention to the subsequent issuance and implementation of supplementary review standards.

2. Brief Review of Provisions on Administration of Security Vulnerabilities in Network Products

Authors: Kevin DUAN | Angus XIE

On July 12, the Ministry of Industry and Information Technology ("**MIIT**"), the Cyberspace Administration of China ("**CAC**") and the Ministry of Public Security jointly promulgated the *Provisions on Administration of Security Vulnerabilities in Network Products* (the "**Provisions**"), which will come into effect as of September 1, 2021. These provisions add new rules for cybersecurity—a field that has recently attracted much attention.

According to the Provisions, CAC will be responsible for coordinating the supervision of network product security vulnerabilities, MIIT will be responsible for the comprehensive supervision of network product security vulnerabilities as well as the supervision and management of network product security vulnerabilities in the telecommunications and Internet industries, and the Ministry of Public Security will be responsible for the supervision and management of network product security vulnerabilities and take actions against illegal and criminal activities committed by taking advantage of network product security vulnerabilities in accordance with the law.

The Provisions will apply to network product providers (including hardware and software products), network operators, and organizations or individuals that engage in the discovery, collection, and publication of information regarding network product security vulnerabilities. The Provisions stipulate legal obligations for these three categories of persons subject and relevant consequences for violating those obligations. Further, the Provisions also prohibit other organizations and individuals from engaging in any activities that involve: endangering cybersecurity by taking advantage of network product security vulnerabilities; illegally collecting, selling, or publishing information on network product security vulnerabilities; or providing technical support, advertising, or settlement services to entities that engage in activities that endanger cybersecurity by taking advantage of network product security vulnerabilities.

Given the *Measures for Cybersecurity Review (Revision Draft for Comment)*, which emphasize a notification regime for cybersecurity review and considers the risk of data leakage, theft, and damage potentially arising from data processing activities, the Provisions, in relevant part, provide a strong reference for enterprises to conduct internal reviews and benchmarking in view of cybersecurity reviews. (For more insights, please see *Analysis of Revised Draft Cybersecurity Review Measures* on page 3).

In the table below we summarize the relevant provisions of the Provisions that apply to each category of persons subject:

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
Network product providers	Establish a reward mechanism for providing network product security vulnerabilities and give rewards to any organization or individual that discovers and notifies of network product security vulnerabilities.	■ Establish and maintain open channels for receiving reports on security vulnerabilities in network products, and keep logs of reported security vulnerabilities for no less than six months; ■ Upon detection or becoming aware of security vulnerabilities in provided network products, immediately organize to verify suspected vulnerabilities, assess the extent of damage and scope of impact, and organize to rectify such vulnerabilities in a timely manner; ■ File relevant security vulnerabilities within two days with the Network Security Threat and Vulnerabilities Information Sharing Platform of the Ministry of Industry and Information Technology; ■ Notify the relevant upstream providers if there are upstream products or components that have security vulnerabilities; ■ Notify downstream users (including downstream manufacturers) of potential security vulnerabilities and rectification methods and provide technical support if it is necessary for product users (including downstream manufacturers) to take	■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY50,000 to CNY500,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cybersecurity; ■ The person directly in charge shall be subject to a fine of CNY10,000 to CNY100,000.

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
		remedial measures such as software and firmware upgrades.	
Network operators		■ Establish and maintain open channels for receiving reports on network security vulnerabilities, keep logs of reported security vulnerabilities for no less than six months; ■ Upon detection or becoming aware of any security vulnerabilities in networks, information systems and equipment, take immediate measures to verify such vulnerabilities and repair the same in a timely manner.	General network operators: ■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY10,000 to CNY100,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ The person directly in charge shall be subject to a fine of CNY5,000 to CNY50,000; Critical information infrastructure operators: ■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY10,000 to CNY1,000,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ The person directly in charge shall be subject to a fine of CNY10,000 to CNY100,000.
Organizations or individuals engaged in activities such		■ Establish a platform for collecting network product security vulnerabilities and file the platform with MIIT; and ■ Establish and maintain open channels for	■ Be ordered to make corrections and given a warning; ■ Be imposed with a fine of CNY10,000 to CNY100,000 if they refuse to make

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
as discovering, collecting and disclosing security vulnerabilities in network products		receiving reports on security vulnerabilities in network products, and keep logs of reported security vulnerabilities for no less than six months; ■ Strengthen internal management and take measures to prevent the leakage and unlawful disclosure of vulnerability information; ■ Publication of vulnerability information to the public through network platforms, media, meetings, contests or otherwise shall be consistent with principles of necessity, authenticity, objectivity and conducive to the prevention of cybersecurity risks; and ■ Shall not publicize vulnerability information before the network product provider takes measures to rectify the security vulnerabilities in the network products; if it is deemed necessary to publicize such information in advance, negotiate and cooperate with the network product provider to conduct a joint assessment, and report the same to the MIIT and the Ministry of Public Security, which shall be responsible for the publication of such information after assessment; ■ Shall not publicize details of security vulnerabilities in networks, information	corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ Be ordered by the competent department to suspend the relevant business, cease business for rectification, close websites, and revoke relevant business permits or business licenses; ■ The person directly in charge and any other person directly liable shall be subject to a fine of CNY5,000 to CNY50,000.

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
		systems, and equipment that are currently in use by network operators; ■ Shall not deliberately exaggerate the hazards and risks of security vulnerabilities in network products, and shall not conduct illegal or criminal activities by using the information of security vulnerabilities in network products, such as malicious speculation, fraud, extortion, etc.; ■ Shall not publicize or provide programs and tools specifically for use in activities that endanger cybersecurity by taking advantage of security vulnerabilities in network products; ■ Shall publicize security vulnerability remedial or preventive measures at the same time when publicizing security vulnerabilities in network products; ■ Shall not publicize security vulnerabilities in network products during major national events without the approval of the Ministry of Public Security; and ■ Shall not provide undisclosed information about security vulnerabilities in network products to overseas organizations or individuals other than to the network product provider.	

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
Other organizations or individuals	■ Notify network product providers of security vulnerabilities in their products; ■ File security vulnerabilities information of network products with the Network Security Threat and Vulnerabilities Information Sharing Platform of the Ministry of Industry and Information Technology, the Vulnerabilities Platform of the National Network and Information Security Information Notification Center, the Vulnerabilities Platform of the National Computer Network Emergency Response Technical Team/Coordination Center, and the Vulnerabilities Database of the China Information Security Assessment Center.	■ Shall not engage in activities endangering cybersecurity by using security vulnerabilities in network products; and ■ Shall not unlawfully collect, sell or publicize information of security vulnerabilities in network products; and ■ Shall not provide technical support, advertising and promotion, payment or settlement services or any other assistance to any other person who they know to be using security vulnerabilities in network products to engage in activities that endanger cybersecurity.	**Where the case does not constitute a crime:** ■ Be confiscated of illegal gains, detained for fewer than 5 days; may concurrently be subject to a fine of CNY50,000 to CNY500,000; ■ In serious cases, be detained for 5 to 15 days and subject to a fine of CNY100,000 to CNY1,000,000. **Where an entity commits any of the acts specified in the preceding paragraph:** ■ Be confiscated of illegal gains; ■ Be subject to a fine of CNY100,000 to CNY1,000,000; ■ The person directly in charge and any other person directly liable shall be penalized in accordance with the provisions of the preceding paragraph. **Relevant personnel:** ■ Any person who has been subject to public security administration penalty shall not serve in key positions concerning cyber security management and network operation within 5 years; and ■ Any person who has been subject to criminal penalty shall not serve in key positions concerning cyber security management and network operation for life.

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
Hong Kong	**Dafei CHEN**	**Attorney-at-law**
	Tel:	+852 2820 5616
	Email:	dafei.chen@hankunlaw.com