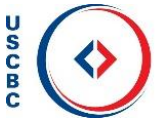
U.S. CHAMBER OF COMMERCE



THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

American Chamber of Commerce in China, American Chamber of Commerce Shanghai, American Chamber of Commerce South China, U.S. Chamber of Commerce, and the US-China Business Council

Joint Submission to the Cyberspace Administration of China

on the

Draft Measures for the Security Assessment of Cross-Border Personal Information Transfers

July 2019

The American Chamber of Commerce in China (AmCham China), the American Chamber of Commerce in Shanghai (AmCham Shanghai), the American Chamber of Commerce in South China (AmCham South China), the U.S. Chamber of Commerce (U.S. Chamber), and the US-China Business Council (USCBC) appreciate the opportunity to submit comments to the Cyberspace Administration of China (CAC) on the *Draft Measures for the Security Assessment of Cross-Border Personal Information Transfers*. We commend the CAC for ensuring regulatory transparency—including opportunities for public comment—during the drafting process.

Our joint submission has two sections: 1) General comments and questions on the draft measures as a whole, and 2) Specific comments on an article-by-article basis.

General Comments

On one hand, China is home to one of the world's most dynamic digital economies, with a world-class research and development (R&D) ecosystem that is capable of producing some of the world's leading technologies. It constitutes a significant market opportunity for American technologies, products, and services. On the other hand, China's digital economy has become increasingly restrictive and difficult to navigate for our member companies. Data localization requirements, prescriptive security requirements, preferences for domestic technology, and restrictions on data security and cross-border movement of data and information continue to pose immediate and far-reaching challenges for many American companies. Our organizations continue to urge China to promote policies that foster openness, clarity, and conform with international standards in China's digital economy.

The *Draft Measures for the Security Assessment of Cross-Border Personal Information Transfers* (Draft Measures) aim to safeguard "Personal Information security, cyberspace sovereignty, national security, and social public interests." We recognize China's need and sovereign right to continue to develop its data privacy framework and to protect the legitimate rights and interests of its citizens and legal persons. We also believe that it is important to affirm that data collection, processing, and cross-border transfers of information and data are an essential element of normal business operations. Consequently, we urge the government to strike a more business-oriented balance between the two. With respect to the Draft Measures, however, we have the following general comments, questions, and concerns:

Comment: Requirements for security assessments prior to cross-border transfers of Personal Information may dis-incentivize foreign investment in China.
The procedural costs for complying with CAC's requirement for pre-transfer security assessments and provincial CAC approval of cross-border transfers in the Draft Measures promise to be onerous, time-consuming, unnecessarily high, and inconsistent with international standards and best practices, such as the APEC CBPRS and the OECD Privacy Guidelines. The overall objective should be to encourage and support the adoption of information security safeguard mechanisms, but the Draft Measures as written would instead promote the drafting and filing of complex and expensive contracts and analysis to complete cross-border Personal Information transfers. If enacted in their current form, the Draft Measures would have a serious adverse effect on the development of electronic commerce both across

borders and in China . Many Articles are characterized by overly broad definitions, vague requirements, and unclear operational guidelines, and present regulatory authorities with excessive discretion with respect to implementation and enforcement.

In order to comply with the Draft Measures, companies will likely be faced with the difficult decision of localizing data processing operations in China or limiting investment in the market due to burdensome compliance obligations and costs. Moreover, we anticipate the Draft Measures will also create a filing and review system so extensive that it could overwhelm the government and make it nearly impossible to complete the assessment procedure in time to meet business needs. We instead strongly recommend establishing a presumption that all outbound Personal Information transfers are pre-approved, and only after an audit by Chinese authorities—given reasonable advance notice—that determines the existence of excessive risk should government approval be required for a specific entity. Alternatively, the draft measures could allow companies to conduct their own security self-assessments that, in conjunction with Personal Information subject's own consent, would suffice for securing cross-border transfers. This would reduce compliance burdens on companies and ensure the long-term, healthy development of China's innovative digital economy.

Along these lines, a system of pre-clearance of those destination jurisdictions that offer sufficient data protections could be adopted. Cross-border transfers that use pre-approved security technology should not be required to undergo a security assessment. Akin to the Adequacy Concept adopted by the European Union, this system could also involve countries that have an adequate legal framework and advanced technological infrastructure. Network operators and recipients whose security practices and profile have been "pre-approved" by an accreditation agency should also not have to undergo a further security assessment and could also be subject to pre-clearance. . Qualified information security consultants should be allowed to conduct the security assessments rather than a government agency to conserve governmental resources, and a certification of approval by such an information security consultant should be accepted as though a security assessment had been conducted and approved by the government itself.

Alternatively, to reduce unnecessary administrative burdens, the draft measures could require only use of a CAC-approved standard contract between the sender and recipient that covers transfers of Personal Information. An existing model for reference is the EU's approach to personal data protection. Under this approach, which does not mandate specific information security provisions, the recipient either agrees to abide by a set of general data protection principles (if the recipient will be processing the data for its own, independent purposes), or the sender and recipient agree in the contract on a set of "reasonable and appropriate" security measures (if the recipient will be processing the data solely on behalf of the sender).

Question: Do the draft measures replace the April 2017 "Measures for the Assessment of Personal Information and Important Data Exit Security"?
In April 2017, Chinese authorities released draft *Measures for the Assessment of Personal Information and Important Data Exit Security* (April 2017 Draft Measures). The April 2017 Draft Measures cover "Personal Information and important data outbound transfer security assessments" that were designed to implement Article 37 of the *Cybersecurity Law*, which requires that "Personal Information and important data" gathered or produced in China by "critical information infrastructure operators" be stored in China.

The contents of these June 2019 Draft Measures seem to overlap with contents from the separate April 2017 Draft Measures without explicitly nullifying, overriding, or replacing them. This creates uncertainty for businesses seeking to comply with China's data privacy regime. We recommend that CAC clarify the status of the various draft measures regulating data privacy and provides a roadmap for publication and finalization of all contents.

We also present several questions of a general nature for which we request that CAC provide responses:

Question 1: Why do the draft measures apply to "Network Operators," when the Cybersecurity Law's rules on data localization apply to the more narrow category of "critical information infrastructure operators"?
The Draft Measures draw their legal authority from the *Cybersecurity Law*, which specifies two categories of regulated entities: Network Operators and critical information infrastructure (CII) operators. With respect to outbound transfers of data, the *Cybersecurity Law* only prescribes responsibilities to CII operators—not Network Operators.

In the Draft Measures, "Network Operator" is defined as "network owners and managers, and network service providers," a definition that is much broader than a CII operator. If a security assessment is required, we recommend narrowing the scope of entities required to undergo the security assessments for outbound transfers of personal data from Network Operators to a narrowly defined set of CII operators.

Question 2: Do CAC and its provincial cyberspace administration possess adequate resources to sufficiently monitor and implement the draft measures?
The draft measures delegate significant authority to provincial cyberspace administration in China to approve outbound transfers of Personal Information. Given the number of companies in China and amounts of data likely collected in the normal course of business operations, the burden for CAC and its authorities to approve each outbound transfer of personal data seems to be significant. The delegation to provincial cyberspace administration also significantly increases the risk of inconsistency in practice between these authorities. We recommend establishing a presumption that all outbound Personal Information transfers are pre-approved, and only after an audit by Chinese authorities—given reasonable advance notice—that determines the existence of excessive risk should government approval be required, thus reducing the administrative burden placed on Chinese authorities to review and approve information transfers.

Question 3: Do these regulations apply to both "data controllers" and "data processors?" There is no clear distinction regarding these roles provided in the Draft Measures.
The Draft Measures frequently refer to "recipients" of Personal Information transfers without distinguishing between the roles of "Personal Information controllers" and "Personal Information processors." Consequently, it would seem as if Personal Information processors are required to assume obligations of Personal Information controllers under the Draft Measures, which could create a number of onerous administrative and compliance burdens. Furthermore, the requirement to provide third-party beneficiary rights to individual

Personal Information subjects (Article 13(3)), which enables them to bring direct claims against the Personal Information recipient renders Personal Information processors legally liable to their Personal Information subjects, a stance which exceeds most international standards, even those in the European Union's General Data Protection Regulations (GDPR). The lack of a clear distinction between Personal Information "controllers" and "processers" also appears to be inconsistent with Article 8(1) of the *Information Security Technology - Personal Information Security Specification (GB/T 35273—2017)* which distinguishes between "data controllers" and "delegated persons", and defines their respective roles and responsibilities. We recommend that the Draft Measures clearly define and distinguish the obligations of Personal Information controllers and data processors.

Article-Specific Comments

The table below reflects comments from member companies across our five organizations:

Article	Comment	Recommendation
Article 2	1) China's Cybersecurity Law only requires operators of CII to complete a security assessment to transfer Personal Information outside of China—not **ALL** Network Operators. Ensure that Article 2 requirements for security assessments of outbound transfers of Personal Information apply only to CII operators. 2) Article 2 states that the Draft Measures apply to all Network Operators who "provide" Personal Information collected in the course of operations within the mainland territory of the People's Republic of China. It is unclear what "provide" means in this context. 3) Article 2 also states that Personal Information that could "affect national security, hurt the public interest, or have difficulty effectively protecting the security of individuals" may not be transferred overseas. "经安全评估认定个人信息出境可能影响国家安全、损害公共利益，或者难以有效保障个人信息安全的，不得出境。"	1) We recommend amending Article 2 as follows: Operators of Critical Information Infrastructure (CII) that collect Personal Information in the course of normal operations in the mainland territory of the People's Republic of China and provide that information to recipients overseas (hereinafter referred to as cross-border transfers of Personal Information) shall conduct security assessments in accordance with these Draft Measures. 2) Clarify what "provide" means in the context of Article 2 for Network Operators. 3) We recommend providing additional clarity on, or examples of, Personal Information that would "affect national security, hurt the public interest, or have difficulty protecting the security of individuals" if transferred overseas. As written, these terms are vague and could permit cybersecurity regulators to make adverse determinations about cross-border transfers based on unknown criteria.

Article	Comment	Recommendation
	It is not clear what kinds of Personal Information would affect national security if transferred overseas. 4) Does "transferred abroad" include Hong Kong, Taiwan, or Macau? Does the term also apply to cases in which an overseas recipient is provided access to Personal Information, but the actual data is not moved overseas? 5) Article 2 has a number of implications that are unclear in the draft measures in its current form: • A certain set of information security standards will have to be formulated and designated as mandatory, and Network Operators will have to meet these standards in order to be permitted to transfer Personal Information outside of China. • The imposition of mandatory security standards could become part of a trend under which China adopts an ecosystem of operating standards that is different and distinct from those used in other parts of the world. Network operators would have to choose between using the ecosystem of operating standards and platforms used in China, and those used in other parts of the world. The result of which would be the "Balkanization" of operating standards around the world with adverse consequences on international business operations for companies from every country. • There is no exception or threshold that applies to the cybersecurity assessment requirement. This will create operational delays for Network Operators, especially if the volume of Personal Information to	If the application for a security assessment includes an opinion from a prior security assessment (or a certificate from a qualified organization) evidencing that the cross-border transfer would not impact national security or harm the public interest, or that it is not difficult to effectively assure the security of the Personal Information, the proposed transfer should automatically pass the security assessment. Personal information that can harm national security if transferred overseas should be limited to a narrow set of clearly defined criteria. 4) Clarify the definition of "transferred abroad," with respect to Hong Kong, Taiwan, Macau. Additionally, clarify if an overseas recipient can gain access to the Personal Information if it is not transferred overseas. 5) China should adopt and enforce a set of security standards that are consistent with international benchmarks or international best practices. China should specify exceptions to the security assessment requirement for cross-border transfers of Personal Information for purposes of internal management of an enterprise. 6) Clarify how Article 2 of the Draft Measures for interplays with Articles 27 and 28 of the draft Data Security Management Measures. Allow Network Operators to pass the security assessment by showing that they have already satisfied

Article	Comment	Recommendation
	be transferred is minimal or not particularly sensitive. 6) It is unclear how the security assessment requirement in these Draft Measures relate to assessment requirements specified in articles 27 and 28 of the Data Security Management Measures draft, or if a successfully completed risk assessment would satisfy the requirements in both draft regulations.	international benchmarks, or already have international best practices in place.
Article 3	1) This Article needs to clarify whether the Network Operator should merely report its cross-border transfer in order to apply for a security assessment before it may proceed with the cross-border transfer, or whether it must actually conduct and pass the security assessment before proceeding with the transfer. If the latter, the compliance burden and strategic costs of conducting a security assessment for all Personal Information outbound transfers by Network Operators will be excessively high. The government is likely to be overwhelmed by the sheer volume and complexity of applications for cross-border transfers. The Chinese economy is huge and already highly digitalized. Requiring that each security assessment be completed and passed before the underlying cross-border transfer may proceed will paralyze international exchanges of information, and therefore will paralyze China's international business relationships and could potentially dis-incentivize certain investments in China. 2) A series of exemptions should be established. The omission of a list of jurisdictions that offer sufficient data	1) We recommend removing Article 3 (in conjunction with Articles 5 and 9) and any requirements for Network Operators to receive government approval for outbound transfers of Personal Information collected in China. Passing a security assessment should be not be a condition for proceeding with a cross-border transfer of Personal Information. Rather, failing a security assessment should trigger a right on the part of the government to order the halt of a cross-border transfer that has already been freely initiated. If Article 3 is to remain, we recommend modifying it such that it is applicable only in a limited number of situations when certain thresholds are met, including: a) CII operators only (as mandated in Article 37 of the Cybersecurity Law). b) Network operators without sectoral regulators, c) Network Operators with a "history" of failing to protect Personal Information,

Article	Comment	Recommendation
	protections and are subject to pre-clearance " from the Draft Measures is puzzling. 3) This Article should specify whether it applies to a Network Operator's head office in China, its local branches, or both. For companies that have branches in many provinces and cities, it is unclear whether the head office would be able to submit a declaration encompassing all of its China operations, or if branches in each region would need to submit declarations to their provincial cyberspace administration separately. 4) The definition of "recipient" is not clear, nor are references to "different recipients" or the "same recipient." Does "recipient" refer to: a) An entity outside of China that could or will receive the Personal Information, b) b) The country that receives the information, c) c) A third party that may receive Personal Information (e.g., a processor or another third party), or d) d) Some combination of these entities? Multinational companies often have multiple branches in different countries, and Personal Information may be used by different branches in different countries within the corporation. In this scenario, is each branch considered a different recipient?对于跨国公司内部企业，在不同国家有多个分支机构，个人信息可以由公司集团内不同国家的不同分支机构使用。 在这种情况下，每个分支是否视为不同的收件人或同一收件人？	d) Large, one-off transfers meeting certain criteria, such as the number of information subjects involved in the transfer, and e) Transfers that meet certain risk-based criteria. We also propose automatically exempting the following from security assessments: a) Data or information that is internal or generated through enterprise production and operation, b) Publicly available information, c) Non-sensitive personal information such as business contact information, d) Employee data to offshore affiliates or the parent company. This is particularly important and makes practical and operational sense to allow free cross-border transfers of employee Personal Information, e) Information shared between entities of the same group where appropriate intercompany arrangements are in place, and Urgent and incidental cross-border transfer of Personal Information, such as for the protection of others' life and property or for the purpose of complying with laws, regulations or court orders of another jurisdiction. 2) An exemption should also be available in relation to overseas jurisdictions and/or transfer mechanisms that offer sufficient data protections and are not required to undergo a security assessment. The CAC should approve particular technological information security mechanisms and make these mechanisms public. Any

Article	Comment	Recommendation
	5) Many of our member companies with operations in China do not maintain offices in provincial capitals. CAC should consider granting local/county-level CAC offices approval authority. 6) We are concerned that redundant written applications for security assessments need to be made for provisions of Personal Information to different recipients. Separate applications for security assessments should not be required for provision of Personal Information to different recipients that are affiliates (under the same control, or under the control of the other party), or which have similar risk profiles, or for provision of Personal Information from different entities within the same group to the same recipient. 7) The requirement to update the approval from the CAC every two years and/or when there has been a change to the purpose, type, or storage of cross-border transfers of Personal Information is duplicative and will likely only create unnecessary administrative burdens. 8) What criteria will be established and how can security assessments be conducted to ensure they are consistently implemented nationwide? There is little detail regarding the security assessment forms/procedures in the Draft Measures. As this assessment will be conducted by the 'provincial-level cybersecurity and informatization department', without standard nationwide procedures/forms the assessment operations may vary by province and create challenges for Network Operators with multiple presences in different provinces.	proposed cross-border transfer that employs one (or perhaps more than one) of the mechanisms on the list should be permitted to proceed without having to undergo a security assessment. The series of approved mechanisms could also involve countries that have a sufficient legal framework and advanced technological infrastructure, and Network Operators and recipients that have been pre-cleared for their security practices and profile by an accreditation agency. Any clearance list could include three sections: a) pre-cleared security technologies, b) pre-cleared destination countries, c) pre-cleared Network Operators and recipients. A cross-border transfer that meets all three sections would then not have to undergo a security assessment. This would be a rational and cost-effective way to promote the actual adoption of security safeguards. 3) Again, we recommend removing any requirements for Network Operators to receive government approval for outbound transfers of Personal Information collected in China. However, if Article 3 must remain, we urge the government to clarify whether Article 3 applies to the head office or local branches of a Network Operator and if the head office can submit a declaration on behalf of all of its branches in China. We also recommend allowing Network Operators to submit a single security assessment declaration to CAC if it has

Article	Comment	Recommendation
	9) Clarify the term "outbound transfer." Is a company that uses a global internal network (such that the data never leaves the company firewall and is subject to no external/third party exposure) covered if the company network is available from within mainland China? 需要对"跨境流动"有更明确的说明。 如果公司网络可以从中国大陆获得，那么公司是否使用全球内部网络（数据永远不会离开公司防火墙，没有外部/第三方暴露）？ 10) The *Information Security Technology-Personal Information Security Specification* states that sharing or transfer of personal information is subject to lesser restrictions if such information is de-identified. We recommend that the Draft Measures take a similar approach to either exempt the cross-border transfer of de-identified personal information from security assessment or design a simple, fast-track manner to assess the transfer of such de-identified information.	used the same contract language with each of its different Personal Information recipients. 4) Clarify the definition of "recipient," "different recipients," and "same recipients," and how these apply to multinational corporations with branches in different countries. We recommend allowing the offshore parent company to sign contracts on behalf of domestically affiliated companies to conduct a one-time assessment rather than requiring all affiliated companies to sign contracts with the recipient and undergo assessments independently. 5) We recommend allowing companies to submit their Personal Information outbound transfer security assessments to local-level CAC offices. CAC could also provide an annex to the Draft Measures with the contact information for provincial cyberspace administrations. 6) Qualified organizations should be permitted to evaluate and certify an organization's security profile, as well as the risk profile of particular cross-border transfers of Personal Information. These organizations should be permitted to issue certificates verifying the security of a proposed cross-border transfer. The Network Operator should be allowed to submit that certificate as part of its report and application for a security assessment. This will relieve the government of the burden of conducting security assessments of each and every cross-border transfer.

Article	Comment	Recommendation
		International examples should be consulted with respect to exemptions for security assessments of cross-border data transfers, for instance: • Article 49 of the EU GDPR • Alternatively, both parties could establish a contract to which the data subject is a party and would benefit. Such a contract would: uphold the public interest; exercise or defend a legal claim; protect the vital interests of the data subject; or the legitimate interests of the Network Operator. 7) We recommend deleting the requirement to have a new security assessment every two years if there has been no change to the purpose, type, or overseas retention period related to the outbound transfer of Personal Information. If the " two-year requirement" remains, China should provide more clarity on what types of changes will trigger the reassessment and allow a risk-based time period for reviews of self-assessments to be determined by the company based on its own risk assessments. Clarify the meaning of "purpose," "types," and "retention period" of cross-border transfer of Personal Information. We also recommend promulgating nationwide criteria regarding the format, structure, and form of the security assessment to reduce the potential for inconsistencies at the provincial level. 8) If the application for a security assessment includes an opinion from a prior security assessment (or a

Article	Comment	Recommendation
		certificate from a qualified organization) evidencing that the proposed recipient is an affiliate of the prior recipient, or that the proposed recipient has a similar risk profile as the prior recipient (for instance, if it has installed the same security safeguard mechanisms and/or maintains the same kind of information security practices), the proposed transfer should not be subject to additional security assessments. If entities within the same corporate group are making the same transfer of Personal Information to the same recipient, those transfers should be reviewed and approved on a consolidated basis by a designated provincial CAC office. 9) Provide a more detailed definition of "outbound transfer" and include descriptive scenarios that help define the scope. 希望有对范围和使用场景有进一步说明. 10) We recommend exempting cross-border transfers of de-identified personal information from security assessment. Alternatively, we recommend designing a simple, fast-track manner to assess the transfer of de-identified information.
Articles 4 & 13	1) Articles 4 and 13 require that Network Operators provide provincial CAC authorities a copy of the contracts signed with data recipients in their declaration of a Personal Information outbound transfer security assessment. Disclosing proprietary details of contracted agreements between private entities presents a competitive risk for companies.	1) We recommend limiting disclosure requirements to high-level details of the receiving entity without requiring disclosure of the competitive nature of agreements. The draft measures should not require precise text that must be used verbatim in the contract, as, for example, is required for contracts used in the European Union.

Article	Comment	Recommendation
	2) Article 4(1) requires submission of a "Declaration Form." Where and when will the form be available? 3) Article 4(2) requires that a copy of the contract between the Network Operator and the recipient should be provided. Where overseas recipients are involved, the contract may be written in a language other than Chinese. CAC should consider approving language that can be used to create and enforce a contract at one time, subject to re-approval after a period of time. For example, if a Network Operator uses 3 different, standardized contract templates A, B and C, the CAC would approve these templates once a year. The Network Operator is then eligible to use these contracts without separate approval so long as the contract template remains unchanged. The requirement to submit a copy of the contract also puts proprietary information at risk and creates issues between the operator and third-party vendors to whom the operator owes confidentiality obligations by requiring parties to divulge commercially sensitive information. 4) Article 4(3) states that Network Operators must provide reports analyzing the security risks and security measures associated with the outbound transfer of Personal Information. This requirement is of concern because IT security measures usually include a company's confidential information. 5) Considering that many multinational companies store their data in a variety of locations and have diverse data storage operating procedures across their many affiliates,	The Draft Measures should require only that the contract cover only particular generally stated subject matter, and that the contract will pass the security assessment so long as it protects the interests of Personal Information subjects in a reasonable manner under these clauses. 2) Provide a copy of the Declaration Form in an annex provided with the final version of the Draft Measures. 希望提供申报表附件，以便网络运营者填写申请安全评估。 3) Clarify whether contracts can be provided in foreign languages to satisfy the requirements of Article 4(2). Consider allowing companies to leave confidential information out of the copies of contracts as part of the materials that they must submit for their security assessments. 4) We recommend deleting Article 4(3). 5) Provide a contract template in an annex with the final version of the Draft Measures. Provide a list of scenarios that detail the rules and reporting requirements for companies performing internal data transfers (within the company). 希望提供合同模板，以便网络运营者和收件人可以填写申请安全评估。界定企业进行内部数据传输的情况下，如何报告以及评估需要哪种支持文件。 6) Provide additional guidance and detail on the documents required for submission, including the

Article	Comment	Recommendation
	can the "recipient" sign a contract with the parent company only? Or is a contract with each affiliate required? Will multinational companies even need to sign a contract with subsidiaries that are legally designated entities of the same company? Requiring multiple contracts will be administratively more difficult. 6) Can the report on the "security risks and security measures" of cross-border transfers of Personal Information be issued by the enterprise itself, or must it be prepared by an external evaluation agency? 7) If a company is using a cloud service provider and the provider has already submitted a security assessment to the provincial cyberspace administration, does this satisfy the requirement for any company using the cloud service? 如果公司使用云提供商并且提供商已经向信息组织提交了安全评估，那么这是否满足使用云服务的任何公司的要求？	report on "security risks and security measures," including whether it must be prepared by an external evaluator and a list of approved evaluators. 7) Clarify third party submission and customer obligations. 需要说明第三方提交和客户义务。 8) We also recommend that CAC only require copies of contract information signed with Personal Information recipients if the recipient is not a subsidiary or affiliate of the Network Operator.
Article 5	1) Requiring approval from CAC (or its provincial offices) prior to transferring **any** Personal Information overseas to foreign recipients will significantly increase administrative burdens imposed on Network Operators. We therefore urge that this Article be revised to narrow the requirement for such approval. If prior approval from CAC is indeed required, we recommend the regulations distinguish between employees' Personal Information and Personal Information of third-party individuals (e.g., customers). Cross-border transfers of employee Personal Information are undertaken to meet	1) We recommend removing requirements for government pre-approvals for outbound transfers of Personal Information (Articles 3, 5 and 9). We recommend that CAC and provincial cyberspace administrations establish a presumption that all Personal Information outbound transfers can occur without restriction, subject to a Network Operator's own self-assessment. Instead, CAC and the provincial cyberspace administration's assessments of outbound transfers should be limited to periodic audits—with reasonable advanced notice.

Article	Comment	Recommendation
	internal management and compliance obligations instead of commercial purposes. Additionally, pre-approval should only be required in special cases (e.g., the cross-border transfer of large volumes of Personal Information, the exact amount of which should be determined in consultation with industry). Consistent with sentiments expressed by the Chinese government over the years committing to allow the market to play a decisive role in business operations, government authorities have made an effort to reduce various pre-approval requirements in favor of less burdensome supervisory mechanisms. CAC should consider similar mechanisms to oversee cross-border transfers of Personal Information. Article 5 also grants provincial cyberspace administration 15 business days (or greater for complex cases) to conduct security assessments after receiving a Network Operator's outbound transfer assessment declaration. This is an excessively long period of wait time for data transfer approvals. Businesses compete in a dynamic global economy where decisions and strategies are often decided in minutes, hours, or days. Restricting timely access to important data may hinder strategic decision making for Chinese and foreign companies, and limit development opportunities in China's digital economy. It is also unclear whether there is a maximum threshold on the extension of the review period. 2) Article 5 does not specify the makeup or process of selection for the experts/members of the technical group conducting CAC's security assessments.	If CAC and its provincial cyberspace administration, through an audit, find fault or excessive risk with an operator's own self-assessments, then we recommend making only that specific entity subject to increased scrutiny. If Article 5 is to remain, we recommend amending it as follows: "After receiving the materials for the cross-border transfer of Personal Information and verifying its completeness, the provincial-level network information department or the county-level network information department shall organize experts or technical forces to conduct safety assessment. The safety assessment shall be completed within 5 working days. Application reviews may be extended on a case-by-case basis but should not be extended indefinitely." Consider specifying a maximum cap on the extension of the review period. We recommend at a minimum specifying a clear time period of review for "complicated cases/circumstances" to prevent reviews extending indefinitely. We recommend clarifying whether the stated 15-day review period includes the time required to "verify the completeness" of the security assessment application, or whether that is a separate matter. If a security assessment is ultimately required under the Final Measures, Article 5 should revise the procedure such that the sender performs the assessment which is then validated by the CAC to ensure it conforms to the

Article	Comment	Recommendation
	3) Is the need to "verify the completeness" of the security assessment submission to the provincial cyberspace administration included within the 15-day limit? 4) Article 5 says assessments will be completed within 15 days after verifying the submission. For any existing applications or in-progress transfers, do we need to retroactively apply for a security assessment? If "yes," during the assessment period, can our business keep running normally?	standards referenced in Article 6, instead of conducting its own assessment 2) We recommend that CAC introduce a transparent and inclusive selection process for establishing its expert/technical groups conducting its security assessments that includes the foreign business community and other foreign stakeholders. 3) For any existing applications or in-progress data transfers that require an assessment, we recommend that businesses be allowed to continue operating normally during the assessment. If the assessment finds a security violation, then businesses should be allowed to take corrective steps without being subject to further delays. 对于正在运行的应用程序或正在进行的事务，给出说明是否需要安全评估。 在评估期间，保持业务运行。 评估完成并显示一些安全问题后，企业需要根据结果进行整改。
Article 6	1) Article 6 states the security assessments for outbound transfers of Personal Information should examine "other content that should be assessed" in addition to other, more specific criteria. "其他应当评估的内容" This catch-all phrase creates regulatory ambiguity and could inhibit the innovative R&D that has contributed so greatly to China's digital economy. In the 21st century global economy, companies conduct research and development across business units, institutions, and teams from around the globe. There is a risk of over-regulating data transfers by including unclear definitions of assessment criteria. This could inhibit the global ambitions of Chinese companies	1) We recommend eliminating the catch-all phrase "other content" ("其他应当评估的内容") from the criteria for which Personal Information outbound transfers are assessed. We also recommend that CAC only require copies of contract information signed with Personal Information recipients if the recipient is not a subsidiary or affiliate of the Network Operator. 2) Provide additional details to clarify what it means to "fully protect" the rights and interests of the Personal Information subjects.

Article	Comment	Recommendation
	and researchers that seek to capitalize on the benefits of global research. 2) The definition of "fully protect" in Article 6(2) lacks clarity. What provisions would meet this requirement and which provisions would not? 3) What is meant by "whether the contract can be carried out effectively" in Article 6(3)? Who is responsible for judging whether the contract has in fact been "carried out effectively?" Would a request for a transfer to a vendor be more likely to be denied if it has previously had a transfer request from a different company rejected? 4) Article 6(4) requires that security assessments focus on evaluating "whether the Network Operator or the recipient has a history of harming the lawful interest of Personal Information subjects, and whether they have ever suffered a major network security incident." The provincial-level cyberspace administrations will be hard-pressed to obtain this information about domestic Network Operators, and evaluate it, within 15 days, but it is unrealistic to assume that it will be able to obtain this information about recipients (who will based abroad) within 15 days, if at all. Would an adverse ruling or finding prosecuted by a data protection authority, a lawsuit settlement, or a consent decree (and subsequent fine/punishment) with the US Federal Trade Commission constitute a "history of abusing the legal rights and interests" of data subjects? The	3) Provide additional details to clarify what it means to carry out a contract "effectively" and who is responsible for or has the authority to make such judgements. 4) If the application for a security assessment includes a certificate from a qualified organization evidencing that the cross-border transfer involves no risk, low risk or an acceptable level of risk, or that the Network Operator has adopted and maintains satisfactory security safeguards and information security practices, the proposed transfer should automatically pass the security assessment. The Draft Measures should only require the provincial-level cyberspace administration report to the central-level cyberspace administration about a security assessment when, as per the second paragraph of Article 7, a Network Operator has objected to the conclusion of a security assessment. If under the final Measures the CAC will still conduct its own assessment, this Article should be amended to make clear that these standards (6(1)-6(6)) apply to both the sender's assessment and the CAC's assessment. Provide guidance on what is expected of Network Operators to determine the recipient's track record with respect to whether they have a history of "harming the lawful interest of Personal Information subjects, and whether they have ever suffered a major network security incident," and whether relatively serious cybersecurity incidents have occurred.

Article	Comment	Recommendation
	proscribed threshold to determine such a "history" is unclear. The scope of a "major network security incident" is unclear. A security incident, for example, may not constitute a breach that requires a company to notify data subjects or regulators. An incident of this nature could simply lead to the relevant security vulnerability being patched or fixed. The provincial-level cyberspace administration is then required to report the status of the security assessment to CAC under Article 7. This will serve only to inundate CAC with huge volumes of information that it may be unable to digest or process on a timely basis. 5) Article 6(5) requires personal information to be obtained in a "legal and proper" manner. As written, this refers to the collection of personal information and does not, as written, apply to outbound transfers of Personal Information. It is not clear what channels are available to assess the legality and legitimacy of personal information acquisitions that do not involve cross-border transfers. 对于第（五）点"获得个人信息是否合法、正当"评估内容，此内容应为网络运营者在收集过程中应满足的，与出境的情况本身并无直接关联。如仅在出境环节需要重点评估，那针对其他不涉及出境的个人信息获取时的合法、正当性是否设有渠道进行评估，并未明确. 6) Article 6(6) requires "other matters" be used in the assessment. Clarification is needed to know what the "other matters" are.	5) We recommend Article 6(5) be removed from the Draft Measures. 建议不将第（五）点"网络运营者获得个人信息是否合法、正当"列入重点评估内容. 6) Clarify what "other matters" in article 6(6) means.

Article	Comment	Recommendation
Article 7	1) The range of potential decisions/conclusions that may be issued by the provincial cyberspace administration is not specifically stated. The range of potential conclusions should be listed, with the corresponding next steps for each to allow Network Operators to effectively implement this Article. 2) If a Network Operator lodges a complaint or would like to appeal a final decision, does such a process have a time limit? Moreover, what are the details for the appeal/complaint procedure?	1) Provide specific details on the range of decisions/conclusions that can be issued by provincial cyberspace authorities, such as "allowed to exit," "conditional exit" and/or "no exit." If conditional exit or no exit is the decision, a justification should be provided. 2) Issue specific procedural details that clarify the materials required and the timeline associated with the resolution of a complaint/appeal filed by a Network Operator, including the contact information of the relevant department with which to file an appeal. We recommend the timeframe be a maximum of 15 days to align with the timeframe for the CAC security assessment in Article 5.
Article 8	1) Article 8 requires records of cross-border information transfers to be retained "for 5 years." The 5-year requirement seems arbitrary and it is not clear on what basis this timeline is justified. 2) Clarify expectations for document transfers of Personal Information. Is each individual's Personal Information transfer record expected to recorded? Or can Personal Information transfer records be grouped/combined/processed together based on business needs? 国家对于记录个人信息转移的管理期望。 是否要跟踪和记录每个单独的传输记录，还是可以根据业务流程和需求对记录进行批量处理？ 3) Article 8 requires detailed recordkeeping that would increase privacy risks.	1) We recommend keeping the cross-border data transfer retention time period consistent with Article 47 of the *Cybersecurity Law*, which mandates a retention period of six months. 2) Clarify these details. 阐明个人信息跟踪级别的期望和说明。 3) We recommend allowing more general documentation that would not increase risk or result in superfluous records.

Article	Comment	Recommendation
Articles 9 and 11	1) Government approval for outbound transfers of Personal Information should not apply to Network Operators and should be limited only to a narrowly defined list of CII operators. 2) The requirement in Article 9 to report annually all cross-border data flows is superfluous and duplicative given that the draft measures already require government-led assessments of cross-border data flows to be re-assessed every two years or upon major changes. 3) It is also unclear how Article 9 interplays with Article 15 of the Draft *Data Security Management Measures*, which requires Network Operators collecting important data or sensitive Personal Information for business purposes to file the matter with the local cybersecurity and informatization department. 4) Articles 9 and 11(1) require Network Operators to report "major" data breaches to provincial-level cyberspace administrations, and that a cross-border transfer of Personal Information may be suspended or terminated in the event of a "major" data breach. • The term "major data breach" or "major incident" must be defined. • Network Operators should not be required to report minor data breaches, i.e., data breaches in which there is no significant likelihood of serious harm to the Personal Information subjects. • The annual reporting procedures and requirements for companies are not clearly laid out in Article 9.	We recommend that Article 9 (in conjunction with Articles 3 and 5) be removed. If Article 9 is to remain, we recommend revising Article 9 as follows: Critical Information Infrastructure Operators shall report their practices regarding the cross-border transfer of Personal Information and the status of contracts to the provincial cyberspace administration before December 31 of each year. 2) We recommend revising the requirement in Article 9 to an internal documentation requirement (a record of processing activities and data flows) to maintain consistency with Article 30 of the GDPR. 3) We recommend limiting the requirement in Article 9 to entities that process important or sensitive personal data as part of their primary businesses or revising the requirement so that companies only have to maintain internal records of processing of activities available for regulatory review, consistent with the requirement in the European Union's GDPR. 4) The term "major data breach" must be defined to help companies understand the scope and their related compliance requirements. Articles 9 and 11(1) should only require Network Operators to report data breaches that involve a substantial likelihood of serious harm to the Personal Information subjects. Network Operators should not be required Network Operator to report minor data breaches, which is to say data breaches in which serious

Article	Comment	Recommendation
		harm to the Personal Information subjects is not substantially likely. Clarify the meaning of and reporting requirements associated with "practices regarding the cross-border transfer of Personal Information," and the "status of performance contracts," as stated in Article 9.
Article 10	1) Article 10 is overly vague in multiple respects. For instance, details regarding the "inspections" to be conducted by the provincial cyberspace administration should be clarified. Will Network Operators be subject to random inspections? What inspection method(s) will be adopted by the regulatory authorities? How frequent will they be? What requirements and workflow are to be imposed on Network Operators by these inspections? 2) The concept of "data leakage incidents" should also be clarified in line with standard legal formulations.	1) We recommend the specification of procedural details on how the examination of "the records of cross-border transfers of Personal Information and other relevant information, with a focus on the implementation of contractual obligations with recipients," and any assessments of a "violation of national rules or any actions damaging the legal rights and interests of Personal Information subjects" will be conducted. 2) We recommend the concept of "data leakage" include the following, which is standard language for these issues: "the unauthorized acquisition of certain computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by the entity that causes a material risk of harm to the individuals whose Personal Information is exposed." The concept should only apply to certain specified sensitive Personal Information, and there should be an exception for good faith acquisition of the information by employees or agents of the company experiencing the breach, where there is no evidence the information has been misused.

Article	Comment	Recommendation
Article 11	1) The definition of "major incidents" and "abused" is not clear. 2) The criteria used to determine whether personal data subjects cannot "protect legal rights and interests related to their Personal Information" is not clear. Similarly, the criteria used to determine whether "the Network Operator is incapable of protecting their Personal Information" is also unclear.	1) & 2) Clarify the definition and details of the following phrases: • "major incidents" • "abused" • "protect legal rights and interests related to their Personal Information" • "protect legal rights and interests related to their Personal Information"
Articles 13-15	1) According to the *Contract Law*, only contracts in violation of mandatory provisions within relevant laws can be voided. Therefore, requiring all parties under contract to be subject to Articles 13-15 is not practical as these Draft Measures are regulations promulgated by a single government agency rather than enshrined in law. Additionally, if these Articles are to be considered best practice, we suggest CAC promulgate a template that provides guidance on how to structure contracts around cross-border transfers of Personal Information. Given the expectation of confidentiality around contracts and the need to maintain some confidentiality around normal business operations, it is not appropriate to allow individuals to request a copy of the contract (Art. 14 (2)) just because one's Personal Information is involved. 2) Article 13(3): data subjects have a legal right to "compensation" if Personal Information is "abused" and are entitled to that compensation unless the Network Operator proves they are not liable. As written, it seems that a mere allegation of abuse is sufficient to require the Network Operator to pay compensation unless they can	1) Delete Articles 13-15 and promulgate a contract template that provides guidance on how to structure cross-border transfers of Personal Information. Consider deeming global businesses who have amended their vendor processing agreements to comply with GDPR to have adequately met the requirements in Articles 13-15. If Articles 13-15 are not to be deleted, we have the following recommendations: 2) Clarify the burden of proof required to trigger a Network Operator's liability, and clarify the criteria for "compensation," as written in Article 13(3). We recommend amending Article 13(3) as follows: "When the data subjects' legitimate rights and interests are harmed, they may claim compensation from the Network Operator, data recipient, or both. If it can be confirmed that the damage came from the Network Operator or data recipient, the Network Operator or data recipient will provide compensation. (个人信息主

Article	Comment	Recommendation
	prove they are not liable, rather than placing the burden on the plaintiff to establish that a violation has indeed occurred in the first place. 3) Article 13(4): How will we assess if it is "difficult to perform the contract?" Who will responsible for making that assessment? 4) Article 14(2) requires a copy of the contract be provided to the Personal Information subject. This is burdensome. These Draft Measures already impose strict regulations on data transfers. Such a requirement will be administratively challenging for contracts that govern the Personal Information of a significant number of subjects. Disclosing contracts to any third party is also inappropriate as business contracts between companies usually contain confidential information. It is unclear if companies have the option of providing only parts of a contract involving Personal Information rather than the entire contract, in order to protect business secrets. 5) Article 14(3): requires Network Operators in China to bear liability for damages caused by third party recipients of Personal Information outside of China. • Article 14(3) is vague and imposes too much liability on the Network Operator. Only large multinational corporations will have the ability to recover from the offshore recipients for damages which they have absorbed on their behalf. Network operators which are SMEs will not have the resources to recover against liabilities incurred by or against offshore recipients. SMEs will see cross-border transfers as a	体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，如能证实损害来自网络运营者或者接收者，则网络运营者或接收者应当予以赔偿.)" 3) Amend Article 13(4) to include performance criteria against which Network Operators and their contractual partners can assess whether the contract can or cannot be filled. Overall, we recommend Article 14 be amended to require Network Operators to provide basic information to individuals about the transfer of their information only if the individual makes a request for such information. Imposing an obligation to provide such detail absent a request will impose a significant administrative burden with minimal if any benefit to most individuals. 4) Recommend deleting Article 14(2) or consider clarifying whether companies can turn over parts of a contract involving only Personal Information rather than the whole contract. Alternatively, revise Article 14(2) to "Provide the necessary materials as required by Article 13 of the Draft Measures." 建议将第（二）点的"提供本合同的副本"修改为提供《办法》第13条所要求的必备条款. 5) If Article 14 remains as written and requires companies within China to bear liability for damages caused by third party recipients, we recommend the Draft Measures only impose liability in the first instance

Article	Comment	Recommendation
	high-risk venture, because they will be exposed to liability to Personal Information subjects within China without having the resources to be able to recover against data recipients abroad. • Only large MNCs will effectively be able to make cross-border transfers of Personal Information. Network operators which are SMEs will be discouraged from making any cross-border transfers. This will serve to exclude SMEs from participation in the international economy and restrict their business opportunities. 6) Article 15(1): requires the recipient to provide access to the Personal Information of the subject at their request in the event of needed corrections/modifications. Given that Network Operators and recipients both have access to the Personal Information, it would be useful to specify the expected procedure for making modifications to the data so that both Network Operator and recipients maintain the correct data. Additionally, Article 15 appears to contradict the *Draft Measures for Data Security Management* currently under consideration, because Network Operators have the obligation to maintain the correct information while recipients are not permitted to make modifications. How should these contradictions be resolved to keep them consistent? Does the term "delete" used in Article 15(1) mean: to "physically delete the data" from database? If so, such requirement would impair the ability of companies to	on Network Operators for damages caused by recipients of cross-border transfers of Personal Information where the recipients are affiliates of the Network Operator. We recommend amending Article 14(3) as follows: "Upon request, relay the Personal Information subject's appeal to data recipients, including demanding compensation from recipient; when a Personal Information subject cannot receive compensation from data recipients, the Personal Information subject can move forward with a claim or the Network Operator can make the compensation first after the occurrence of the damage has been confirmed and the basis of the claim has been validated. (应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，证明损害发生，确定索赔依据之后可进行索赔或主张先行赔付.)" Lastly, we also recommend that CAC only require copies of contract information signed with Personal Information recipients if the recipient is not a subsidiary or affiliate of the Network Operator. 6) Clarify how Article 15(1) can and will be compatible with other regulations and Draft Measures under consideration. If a user requests that its Personal Information to be deleted (Article 15(1)), we recommend the Network Operator or recipients shall instead de-identify the data and make it completely anonymous rather than being

Article	Comment	Recommendation
	maintain a record of their data transfers, as required by Article 8. 7) Article 15(3): The requirement for the Network Operator to report to the competent provincial-level cyberspace administration is overly burdensome and lacks clear objectives. How should Network Operators "report" to the provincial cyberspace administration? What information is required to be reported and in what format?	required to physically delete the data from the database. 如果用户请求删除个人信息，网络运营者或接收者应进行个人信息识别并做出脱敏处理，而不是从数据库中进行物理/彻底删除。 7) We recommend deleting Article 15(3), or if this provision remains, provide details on the structure and content of the "reports" that must be filed with provincial cyberspace administration.
Article 16	1) What is the scope of "third party?" Does it include a subsidiary under the recipient? Does it include a subsidiaries or branches of the recipient based in a third-party location? 2) What is the definition of "transmission?" 3) Article 16(1): Must the Network Operator notify the subject every time Personal Information is transmitted to a third party, or does a notification cover all situations in which information is transmitted to a third party over a certain period of time? 4) Article 16(3): Requires consent by the subject of Personal Information to transmit "sensitive Personal Information" to third parties. Does that this mean that the transmission of other Personal Information (i.e., non-sensitive Personal Information) is not subject to consent of the subjects in accordance with the provisions of the first paragraph of this article? No explicit consent is required? 5) Article 16(4): The Draft Measures require Network Operators in China to bear liability for damages caused by	We recommend Article 16 be amended such that the sole requirement for a subsequent transfer of Personal Information by the data recipient be that the recipient complies with all of the obligations imposed under the agreement for the initial transfer outside of China. The requirement to notify individuals of the transfer of their data by the recipient to third parties is burdensome and unnecessary to protect their interests. Consider deeming global businesses who have amended their vendor processing agreements to comply with GDPR to have adequately met the requirements in Article 16. If Article 16 is to remain in its current form, we have the following recommendations: 1) Clarify the scope and definition of "third party." We recommend specifying that the definition of "third party" exclude the affiliated companies of the recipient. 2) Clarify the meaning of "transmission."

Article	Comment	Recommendation
	third party recipients of Personal Information outside of China. • This imposes too much liability on the Network Operator. (See comment above re: Article 14(3)).	3) Provide details about whether Network Operators need to obtain consent every time Personal Information is transmitted to a third party, or whether consent covers multiple data transmissions. 4) Clarify the details about exactly what kind of Personal Information (sensitive vs. all other types) needs to obtain consent of the subject in order to be transmitted? 5) We recommend the Draft Measures only impose liability in the first instance on Network Operators for damages caused by recipients of cross-border transfers of Personal Information where the recipients are affiliates of the Network Operator.
Article 17	1) Article 17(1) and (3) require the Network Operator to provide in the report a discussion of the background, scale, business, finances, reputation, network security capabilities, etc. of itself and the recipient, as well as an analysis of the risks of the transfer of Personal Information to destinations outside of China. Few Network Operators are in a position to analyze these matters. For that reason, Network Operators are consequently going to need to hire outside consultant(s) to analyze the associated risks stemming from the proposed cross-border transfer, as well as to assess the security safeguard measures, and compile the report. This will incur significant cost. • Does "business" and "financial details" refer to the financial situation of Network Operators and data recipients, and if so, to what extent should the company disclose this information to the network information department?	1) In order to prevent overwhelming the government's resources by requiring it to conduct security assessments of each and every cross-border transfer, and because the Network Operator is already in a position where it must engage an outside consultant to conduct a risk analysis, qualified organizations should be permitted to evaluate the risk profile of particular cross-border transfers of Personal Information, and compile the related report. These organizations should be permitted to issue certificates verifying the security of a proposed cross-border transfer. The Network Operator should be allowed to submit that certificate as part of its report and application for a security assessment. More clarity is needed around the type of information and scope of coverage discussed in this Article. We recommend limiting the required information to

Article	Comment	Recommendation
	• How to assess the "network security capability" of Network Operators and data recipients? On what criteria and by whom? • What details and criteria are to be considered in the risk analysis of Personal Information transfers?	information that is already required to be provided under existing statutes.
Article 18	1) The provisions in Article 18 with respect to violations of these Measures (and by implication other relevant laws and regulations) are excessively broad and vague. 2) It is unclear if there are any differences in penalties applying to Network Operators and CII operators.	1) We recommend providing specific guidelines for addressing violations that have taken place, as well as the associated penalties for Network Operators in violation should be provided explicitly in this Article 18. 2) We recommend limiting the application of Article 18 to CII operators to maintain consistency of the draft measures with the *Cybersecurity Law*.
Article 20	1) The Draft Measures require offshore organizations which collect Personal Information from users in China by such means as the internet to perform the legal obligations and duties of Network Operators under the Draft Measures through a legally designated representative in China. The *Cybersecurity Law* does not explicitly provide for or necessarily have any jurisdiction overseas. Therefore, Article 20 is overstepping its jurisdiction. It is impractical to require a China-based entity or subsidiary to address any legal liability that may arise from the actions/operations of its overseas parent company or head office given that each company is legally independent. Realistically, only multinational corporations with legally designated subsidiaries or affiliates in China will respect this provision. Offshore organizations which are not MNCs will not have an affiliate or subsidiary in China. They will be able	We recommend deleting Article 20. If Article 20 is to remain, then we recommend the requirement that offshore Network Operators perform legal obligations and duties through a legally designated representative in China be amended to apply only to offshore Network Operators that have an actual affiliate or subsidiary in China. Additionally, if Article 20 is to remain, it requires more detailed provisions to help companies understand both the Article's meaning and their ability to comply with the regulations. In particular, we ask that the terms "legal representative (法定代表人)" and "institution (机构)" be clarified.

Article	Comment	Recommendation
	to ignore this provision with impunity. Courts in offshore jurisdictions are unlikely to enforce this provision within their own jurisdictions. Eventually, offshore organizations which are not MNCs will realize that they can collect Personal Information from China over the internet without any fear of prosecution from China, creating a dual system that creates in practice a system that promotes compliance by certain organizations and businesses of a certain size and legal standing, while allowing others to bypass such regulations. 2) Are intra-company (i.e., between the company its legal subsidiaries) covered under Article 20 or are they treated differently? 3) What do "legal representative (法定代表人)" and "institution (机构)" mean? Do these terms refer to the legal representative of the foreign company's wholly foreign-owned enterprise in China? Who would be the legal representative for overseas entities which only have Sino-foreign joint ventures in which the legal representative may be appointed by the Chinese partner or for overseas entities without any legal presence in China?	
Article 21	1) Article 21 defines the terms "Network Operators" and "Personal Information." The definitions are very vague and unclear. For example: • "Network operator" refers to the "owners and administrators of a network, as well as network service providers." What is the scope of network service providers? Does it apply to any company that uses an IT system? Does it include the network	1) Clarify the vague definitions and details around "Network Operators" and "Personal Information" in Article 21. See the Comments for the types of questions that these definitions raise. 2) In the *Information Security Technology-Personal Information Security Specification* specific examples of "sensitive Personal Information" were provided in the document. We recommend the same examples be copied here to

Article	Comment	Recommendation
	used within a company (intra-company system), or does it refer only to public network services accessible to internet users? • Is a customer's internal business data stored on the cloud and not publicly collected via the Internet (e.g., HR info, customer account info) included within the scope of Personal Information and data? • Are cloud operators jointly liable for data transfers made by the customer's through the Cloud? (e.g., VM or container data syncs)? 2) The criteria provided for "sensitive Personal Information" are vague.	provide clarity and also ensure consistency between the Draft Measures and these existing standards.
Article 22	1) Companies should be given a grace period to comply with the draft measures should they be finalized.	1) We recommend a minimum grace period of 12 months before such Draft Measures become effective. Final measures should not apply to cross-border transfers completed prior to the effective date.