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

USCBC Comments on the Draft Outbound Data Security Assessment Measures

November 26, 2021

On behalf of the 260 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the draft Outbound Data Security Assessment Measures.

The draft measures offer greater clarity to the recently implemented Data Security Law (DSL) and Personal Information Protection Law (PIPL). The top 100 foreign companies in China contribute at least 6 percent of China's total GDP[1]. Many of them are multinational companies with globally optimized information technology systems and integrated security policies. Seamless data flow is essential to these companies and is critical for global trade and uninterrupted business operations. Restrictions on cross-border data transfers between these companies, as well as all other foreign companies in China, and their global operations will have substantially negatively impacts on their existing and future investments in China.

At this critical juncture, we recommend that China impose only measures necessary to protect national security, working to limit restrictions that unduly influence the business community. The current draft sets the threshold for cross-border security reviews so low that their scope will likely be overly expansive and unnecessarily impede normal business operations. After careful consultation with members from a diverse range of sectors, we urge the Cyberspace Administration of China (CAC) to consider the following suggestions.

- **Avoid conflation of important data and personal information:** We strongly recommend that CAC align with global practice when it comes to cross-border transfers of personal information and restrict security assessments only to important data. This focused approach will guarantee CAC's administrative resources are directed to truly critical areas, without conflating non-sensitive personal information and important data. We appreciate CAC efforts to decouple personal information and important data in the draft Measures on the Security Assessment of the Cross-Border Transfer of Personal Information (2019) and draft Data Security Management Rules (2019), recognizing the risks associated with the two categories of data are inherently different. We encourage the CAC to continue to decouple regulatory approaches to these two types of data.
- **Focus assessments on business models and not specific transfers:** The scope of outbound transfer assessments is unclear. We strongly encourage CAC to clarify that its outbound transfer assessments are intended to review companies' business/operational models for cross-border data transfers, and that each CAC approval is a 2-year validation for ongoing transfers within the scope of that approval. This clarification would help companies understand that these measures are not intended to scrutinize each single instance of data transfer, creating significant business continuity burdens for companies, but rather allow for ongoing secure transfers within the scope of a model approved by CAC assessment.

[1] According to Hurun Report's 2021 Foreign and Hong Kong Investment Top 100 report.

- **Adjust the review threshold for personal information (PI) processors:** In the draft's current form, Article 4 mandates that processors with 100,000 sets of personal information or 10,000 sets of sensitive personal information undergo a security assessment prior to a cross-border data transfer. This threshold is too low, and stands to unreasonably increase compliance costs, impact administrative resources, and hinder normal cross-border data flows and business operations. In addition, volume is a poor indicator of risk and as such volume based-thresholds do not accurately safeguard cross-border data flows. We suggest the removal of volume-based thresholds to avoid unnecessarily impeding company operations and increasing regulatory workload. If CAC is to retain PI volume thresholds in the draft measures, we recommend that CAC align the scope with the requirements set out in the PIPL (PIPL Article 38 and 40). This would only require CII operators and data handlers handling PI above a set volume (that is less prohibitively low) to localize storage and undergo cross-border security assessment.
- **Propose a practical and limited scope for the definition of cross-border transfer:** The current definition of cross-border data transfer lacks specificity, which is likely to increase operational challenges and unnecessarily expand restrictions. We suggest providing a clear definition of what constitutes a cross-border transfer that explicitly excludes public data, employee data, remote viewing of data, or transfers to Hong Kong and Macau. Alternatively, a fast-track or waiver system for this type of low risk, regular data transfer would facilitate ease of management. Other international agreements may also serve as models for streamlined cross-border data transfer. China is currently pursuing membership of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA). Both agreements include provisions that would allow for non-discriminatory, free flow of necessary business data, including PI, provided that both parties meet relevant legal obligations.
- **Resolve outstanding ambiguities with other regulations:** The draft measures require a security assessment by the CAC and signing a standard contract between sender and overseas data recipient (Article 6). However, Article 38 of the PIPL specifies that only one of three options is required for a cross-border transfer. We recommend aligning the draft measures with the PIPL to avoid unnecessary ambiguity and duplication of regulatory requirements. In addition, when submitting such a contract, we would recommend it be standard practice to sign a non-disclosure agreement between the relevant CAC department and the applicant to protect business confidentiality.
- **Simplify the reassessment process:** Article 12 requires processors to reapply for cross-border data transfer authorization every two years, with a review period between 45 and 60 days. We suggest shortening this review period to two weeks if no substantial changes have occurred, as the current timeframe will impact flexibility and efficiency. We also recommend allowing cross-border data transfers to continue while a review is ongoing and to provide a channel to appeal and seek clarification on CAC decisions should an application be rejected.

Our detailed article-by-article comments are attached in Chinese version of this document.