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

USCBC Comments on the Draft Network Security Management Measures

December 13, 2021

On behalf of the more than 260 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on China's draft Network Security Management Measures. We understand that this regulation is intended to further clarify and explain the requirements under the Data Security Law (DSL), Cybersecurity Law (CSL), and Personal Information Protection Law (PIPL). We welcome strong cybersecurity and privacy standards, as well as efforts to clarify and align with existing regulations for ease of compliance.

However, elements of the draft far exceed existing requirements under CSL, DSL and PIPL. These disparities may result in unintended consequences, particularly with regards to the expanding definition of important data, conflating privacy and cybersecurity, and muddling distinctions between China's key cyber regimes.

- **Disparate legal requirements:** This draft contains duplicative requirements for cross-border data transfer security assessments already outlined within PIPL and expands review requirements to any and all data (Article 35). This expansion of regulatory scope will significantly impact the flow of data, and the definition and review method does not align with PIPL standards. We recommend limiting requirements for security assessment, certification, or signing of a standard contract within Article 35 prior to cross-border transfer to important data or data by processed critical information infrastructure operators. We also recommend releasing a standard contract template in line with the European Union's Standard Contractual Clauses (SCC), ASEAN Model Contractual Clauses (MCCs), or another internationally adopted reference.
- **Important data provisions implicate all data:** The current draft is written such that any data that comes into contact with important data will be subject to a security assessment. This means that regardless of any privacy or data security measures, an organization may be subject to duplicative regulatory supervision. For example, human resources data for employees working on projects with important data could be interpreted as "important" to state interests unless the law explicitly provides legal exemptions.
- **Potential for regulatory overreach:** The draft grants a high degree of control to regulators, meaning that security assessments even for minor errors or omissions provide regulators with access to private sector data. This regulatory approach ignores the other legal and contractual obligations that companies owe to customers.
- **Include a reasonable transition timeline:** Understanding compliance burdens associated with cybersecurity and data management involves a large investment of resources and time. In order to provide sufficient time to clarify and navigate these standards, we recommend a grace period of 18 to 24 months after all applicable important data catalogues are issued.

- **Align with international standards:** We applaud China's active engagement with the cyber and data frameworks within the Digital Economy Partnership Agreement (DEPA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Given China's active participation in global standard setting efforts, we strongly recommend that China recognize and adopt international standards wherever possible, including adherence to the cross-border free flow of data and prohibitions of mandates requiring data be hosted locally. Aligning approaches with international standards that are developed in an open, inclusive, and transparent manner with multiple stakeholders' perspectives will ensure that China's standards are comprehensive and continue to support business growth.
- **Decoupling personal information and important data:** Personal information above a set volume and important data are treated as equivalent within this draft and other relevant regulations. Personal information is different in nature and risk than important data, and privacy standards should be distinct and separate as a consequence. Conflating both terms unnecessarily increases compliance burdens and does not efficiently protect the needs of consumers.
- **Promote the business community as a trusted partner:** We support the promotion of sound data governance practices, including classifying data based on risk. In order to promote the most effective classifications, regulators and the business community should have the flexibility in classifying their own data based on a risk-based approach appropriate to their sector and industry. Given that they serve different purposes, we would recommend that government data and commercial data also be classified separately. For commercial data classification, companies should be permitted to take the lead in determining the appropriate classification levels for data under their control.

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