THE US-CHINA BUSINESS COUNCIL
美中贸易全国委员会

USCBC Comments on the Second Draft of the Data Security Law

May 28, 2021

On behalf of the more than 245 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the second draft of the Data Security Law of the People's Republic of China (hereafter referred to as "the Draft") to the National People's Congress (NPC).

USCBC received comments on the Draft from companies across multiple industries, including information and communications technology (ICT), professional services, and financial services.

We acknowledge the steps the NPC has taken to address concerns mentioned in our comment letter on the previous draft. The second Draft clarifies the central government's role in creating "important data" catalogs and features updated provisions that further align it with the *Cybersecurity Law*. Specifically, the Draft integrates the cybersecurity multi-level protection scheme (MLPS 2.0) into its data security management provisions and affirms the primacy of the *Cybersecurity Law* in matters related to cross-border data flow.

Despite these improvements, many member concerns remain unaddressed and certain attempts to provide clarity have introduced new concerns. USCBC appreciates the complexities involved in regulating data and urges the Chinese government to remove barriers to the free flow of data and ensure the Draft does not impose undue burdens on companies. In particular, we would like to highlight the following suggestions:

1. **Scope and relationship with other laws**: As mentioned in our previous comment letter, the scope of the Draft is overly broad, as it covers any data in electronic or non-electronic forms, potentially capturing any commercial activity related to data. Additionally, there are a number of existing laws, regulations, and standards that already cover some of the national security elements included in the Draft. This includes the *Cybersecurity Law, Civil Code, National Security Law,* the draft Data Security Management Measures, and the draft Measures for the Security Assessment of Cross-Border Transmission of Personal Information. We encourage the NPC to ensure regulatory consistency between the

aforementioned laws and regulations and limit overlap between existing laws and regulations and this Draft. We also suggest limiting the scope of data to be more practically manageable by excluding foreign-sourced data handled in China.

2. **Important data**: We maintain that the Draft could be improved by defining "important data" and "processors of important data" in a way that provides clarity, while limiting the scope and necessity of important data risk assessments. Existing regulations suggest important data will be subject to data localization and cross-border security reviews, so we recommend that the Draft's definition aligns with the draft Data Security Administrative Measures, which state that most company data is not included in the scope of important data. We acknowledge that the NPC has considered feedback and clarified that the central government will define an important data catalog. However, the Draft still empowers each "region and department" to create its own separate catalog, increasing the risk that different provinces and municipalities will have disparate catalogs and compliance requirements, which could impede the free flow of data necessary for companies' day-to-day operations. Therefore, we suggest that the authority to define important data be centralized.
3. **Cross-border data flows**: Article 30 of the revised Draft expands cross-border data flow restrictions for important data beyond the restrictions for critical information infrastructure operators outlined in the *Cybersecurity Law*. Cross-border data flow is important for multinational corporations to communicate with their headquarters and conduct day-to-day business operations such as "know-your-customer" and anti-money laundering activities. The free flow and exchange of data globally supports innovation and the global economy. We, therefore, recommend limiting the cross-border restrictions on important data to CII operators as per the *Cybersecurity Law*.
4. **MLPS 2.0:** We recognize efforts to align the Draft closer with the *Cybersecurity Law* by establishing the cybersecurity multi-level protection scheme (MLPS 2.0) as the baseline framework for the management of data processing activities. However, Article 20 requires the state to establish a multi-level protection scheme for data, suggesting two different data protection schemes. We recommend amending the draft so that it's clear that the state's multi-level protection for data is the MLPS 2.0.
5. **Extraterritoriality:** Article 2 states that the Draft applies to organizations and individuals outside of mainland China that engage in data activities that harm China's national security interest. It is unclear what mechanisms would be leveraged to enforce this provision nor which data activities are considered harmful to China's national security. This contributes to concerns surrounding the increased proliferation of national security-based regulations and reviews in China's data and cyber regulations. Furthermore, companies note that there are

more appropriate laws, such as the National Security Law, to regulate the concern addressed by Article 2. We, therefore, recommend that the Draft's extraterritorial provisions be removed from Article 2.

6. **Oversight**: The government entities responsible for supervision and enforcement of the Draft are unclear, and in some cases may have regulatory overlap, which may cause confusion. In order to avoid duplicative oversight, different government agencies should be clearly assigned respective enforcement and oversight authorities.

We appreciate this opportunity to express our suggestions and have provided article-specific recommendations in detail in the Chinese version.