USCBC Comments on the Draft Revised Cybersecurity Review Measures

July 23, 2021

On behalf of the more than 250 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the draft revised Cybersecurity Review Measures (hereafter referred to as "the draft revisions") to the Cyberspace Administration of China (CAC).

We acknowledge that all countries have legitimate national security concerns regarding the information and communication technology (ICT) supply chain for critical information infrastructure (CII). As an important implementing measure to the *Cybersecurity Law*, the measures provide much-needed guidance on how the Chinese government aims to address these concerns through cybersecurity reviews.

However, the draft revisions stand to increase compliance requirements and ambiguity regarding China's complex cybersecurity regime. They run counter to clarity provided in the original measures, and expand the scope of national security concerns in ways that may unduly burden non-CII operators.

USCBC appreciates the complexities involved in regulating data and ICT products and services and urges the Chinese government to apply cybersecurity reviews in as limited and consistent a manner as possible. In particular, we would like to highlight the following suggestions:

1. **Keep scope limited to CII operators:** In addition to CII operators, the draft revisions would also require data processors to undergo cybersecurity reviews should their activities impact national security. As mentioned in our comment letter on the Data Security Law, the scope of data processing activities is overly broad, making it unclear which data processing activities will trigger a cybersecurity review. This broad scope not only increases uncertainty for business and creates challenges for companies wishing to comply, it would also be unwieldy to implement in a consistent and rules-based manner. Furthermore, the distinction between CII and non-CII operators is unclear, further complicating how companies must approach compliance. We recommend maintaining the original scope of cybersecurity reviews to CII operators as per the original measures.
2. **Delink data and overseas IPO requirements:** Using possession of data as a criteria to determine eligibility for listing on overseas stock exchanges goes against international norms, fails to meaningfully address security risks, and is detrimental to China's technological development. USCBC is not aware of any other nation that uses a company's possession of data as a criteria to list abroad. Furthermore, we are not aware of any US legal requirements that would allow the US government to force Chinese

companies to turn over Chinese user data collected in China solely because they are listed on a US stock exchange. Finally, US capital markets provide Chinese companies access to funds that are important for them to innovate and compete globally. Denying them this stream of investment only serves to limit China's own technological development.

3. **Use risk rather than data volume as a basis for reviews** The draft revisions would require operators with more than 1 million users conducting an overseas initial public offering (IPO) to report to the Cybersecurity Review Office for a cybersecurity review. Our members strongly oppose volume-based compliance requirements, as the amount of data a company gathers in and of itself is not a meaningful indicator of risk. Companies collect many different types of personal information, which carry different levels of risk, including personal information that users self-publish online. We recommend that regulators use risk-based criteria as a basis for cybersecurity reviews rather than volume.
4. **Clarify key terminology:** The draft revisions require that operators adopt measures to protect "important data" and "core data," terms that remain vaguely defined. By mandating provisions around unclear concepts, the revised measures make it more difficult for companies to comply by denying them meaningful ways to understand their responsibilities.
5. **Ensure impartial implementation:** We appreciate the measures' explicit commitment to objectivity in cybersecurity reviews. However, we maintain concerns that the cybersecurity reviews outlined in the draft revised measures could disproportionately burden companies with cross-border operations (including both foreign multinationals and also Chinese companies striving to become globally competitive) and incorporate political and non-trade related risks. American businesses have made significant contributions to China's ICT supply chain and hope to continue to be partners to help China achieve its technological development goals.

USCBC welcomes CAC's engagement with US industry to determine appropriate technical criteria to address national security concerns. Please consider us a resource as China continues to develop its cybersecurity regulatory framework. Please find more detailed suggestions in the Chinese version of this letter.