Global Industry Comments on Draft Data Transfer Assessment Measures

The undersigned organizations, representing companies with business activities or interest in China and other global markets, respectfully submit this letter regarding the draft Security Assessment Measures for Cross-border Transfer of Data (“Data Transfer Assessment Measures”). At the outset, we would like to express our support for the Cyberspace Administration of China’s (“CAC”) efforts to provide clear guidance relating to the data transfer assessments that are referenced in the Cybersecurity Law (“CSL”), the Data Security Law (“DSL”), and the Personal Information Protection Law (“PIPL”), as well as several subsidiary regulations.

The ability to transfer data securely across transnational digital networks is of central importance to the national policy objectives of many countries, including China. Data transfers support COVID-19 recovery, digital connectivity, cybersecurity, fraud prevention, anti-money laundering, and other activities relating to the protection of health, privacy, security, and regulatory compliance.

This ability also supports shared economic prosperity. Cross-border access to marketplaces, purchasers, suppliers, and other commercial partners allow Chinese enterprises in all sectors to engage in mutually beneficial international transactions with foreign enterprises. Data transfers, which are critical at every stage of the value chain for companies of all sizes, support global supply chains and promote productivity, safety, and environmental responsibility.

This ability also supports innovation and transnational research and development (R&D), as well as intellectual property protection and enforcement. Scientific and technological progress require the exchange of information and ideas across borders: As the WTO has stated, “for data to flourish as an input to innovation, it benefits from flowing as freely as possible, given necessary privacy protection policies.”

To avoid prejudicing these priorities, we respectfully submit that the draft Data Transfer Assessment Measures should: (1) not impose greater restrictions on data transfers than necessary; (2) afford equal treatment to Chinese and foreign enterprises, services, and technologies; and (3) be administered in a uniform, impartial, and reasonable manner with a view to ensuring non-discriminatory and streamlined approvals. Additionally, we make the following observations:

- Security assessments should not be mandated for each individual transfer of data, but should encompass a given processing activity or set of activities;
- The requirement under Article 6(3) to submit any “contract or any other legal document” should be narrowed to focus on safeguards pertaining to data transfers. As drafted, it could unnecessarily expose trade secrets and other non-relevant information;
- The draft clauses relating to data processing agreements in Article 9 should be aligned with the “standard contracts” provided for under PIPL Article 38(3). These clauses should also be designed to be interoperable with other global frameworks, such as EU GDPR standard contractual clauses or the APEC Cross-Border Privacy Rules;
• The short validity period of two years for CAC’s security assessments should be extended to avoid creating procedural bottlenecks and undue burdens on the CAC and private enterprises;

• The numerical thresholds under Articles 4(3) and 4(4) as well as the other determinative criteria for data transfer approvals should undergo a thorough review of: (1) whether these thresholds, determinative criteria, and \textit{ex ante} mandatory security reviews are in fact necessary to achieve China’s relevant public policy objectives; (2) whether other less onerous alternatives\textsuperscript{6} could feasibly achieve those policy objectives with fewer data transfer restrictions; (3) the impacts (economic and non-economic) of various alternatives on enterprises and other persons that depend upon the transfer of data; and (4) the grounds for concluding that a particular alternative is preferable to others.

Given the potential consequences for China’s economy and its international economic relations, we also respectfully request that CAC build in more time for robust consultations with the relevant stakeholders and a meaningful implementation period. This not only helps CAC and industry better understand each other’s concerns; it would also allow the industry to put in place adequate processes and procedures to comply with the Draft Measures.

We are grateful for the opportunity to share these perspectives and we look forward to continued engagement with CAC on these matters.

Sincerely yours,

\begin{itemize}
\item 1. ACT | The App Association
\item 2. Africa Information and Communication Technologies Alliance (AfICTA)
\item 3. Africa Cloud Computing Association
\item 4. AmCham China
\item 5. American Council of Life Insurers
\item 6. China Cloud Computing Association
\item 7. Asia Cloud Computing Association
\item 8. Asia Securities Industry & Financial Markets Association (ASIFMA)
\item 9. Associação Brasileira das Empresas de Software (ABES)
\item 10. Australian Information Industry Association (AIIA)
\item 11. BIO – The Biotechnology Innovation Organization
\item 12. BSA | The Software Alliance
\item 13. Center for International Economic Collaboration (CFIEC)
\item 14. Coalition of Services Industries (CSI)
\item 15. Computer and Communications Industry Association (CCIA)
\item 16. Ecommerce Forum Africa
\item 17. European Automobile Manufacturers’ Association (ACEA)
\item 18. European Publishers’ Council (EPC)
\item 19. European Services Forum (ESF)
\item 20. Global Data Alliance
\item 21. Information Technology Industry Council (ITI)
\item 22. TECHNATION Canada
\item 23. US Chamber of Commerce
\item 24. US-China Business Council
\item 25. US Council for International Business (USCIB)
\item 26. US Information Technology Office (USITO)
\item 27. World Information Technology and Services Alliance (WITSA)
\end{itemize}


\textsuperscript{2} Articles 37, Cybersecurity Law

\textsuperscript{3} Articles 30 and 31, Data Security Law

\textsuperscript{4} Articles 38 and 40, Personal Information Protection Law


\textsuperscript{6} Such alternatives could include higher numerical thresholds, less restrictive criteria, or lower frequency reviews. They could also subject fewer classes of transactions to mandatory security reviews.