US-China Business Council Comments on the Draft Data Security Law

August 14, 2020

On behalf of the more than 220 members of the US-China Business Council (USCBC), we appreciate the opportunity to submit comments on the draft 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), automotive, service firms, and financial services.

The Draft covers an important and complex topic that many governments across the world today are debating how to best regulate in a fashion that both ensures the integrity of data protection systems, while not imposing undue or unnecessary burdens on industry. In particular, we would like to highlight the following suggestions:

1. **Scope and relationship with other laws**: The scope of the Draft is overly broad, as it covers any data in electronic or non-electronic forms, making the potential compliance burden for companies difficult. 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.
2. **Important data**: We believe 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 states that most company data is not included in the scope of important data. Furthermore, the Draft 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. **Data classification and MLPS 2.0:** Article 19 of the Draft states that data will be graded and classified according to its importance to China's national security. We recommend that this classification system be harmonized with the existing MLPS 2.0 scheme to avoid the proliferation of different national security-based compliance regimes that companies will be subject to.
4. **Personal information and data:** The Draft's broad definition of data makes it unclear whether it is inclusive of personal information. As per the Cybersecurity Law, personal information and important data are separate concepts that have thus far been regulated separately by standards and regulations. Including personal information in the Draft's definition of data would run counter to existing regulations and complicate companies' present understanding of their compliance requirements. We recommend that the Draft explicitly exclude personal information from its definition of data to ensure consistency with existing laws.
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 removing this provision.
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.
7. **Cross-border data flows**: Cross-border data flows are 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 are encouraged that Article 10 of the Draft commits to promoting free data flow. Members hope to see clarity on how cross-border data security will be balanced with the need for unencumbered cross-border data flow.

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

List of Comments			
Article #	**Article/Clause**	**Comments**	**Suggestions**
Chapter 1	General Principles		
2	This Draft is applicable to the conduct of data activities within the mainland territory of the People's Republic of China. Where organizations or individuals outside of the mainland territory of the People's Republic of China engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations of the People's Republic of China, legal liability will be investigated	1)The first sentence of Article 2 states that the Draft applies to data activities within the PRC, yet the first sentence of the second paragraph refers to activities conducted outside of the PRC. 2)The conditions under which the extraterritorial elements of this article apply are vague and broad. 4) It is unclear how authorities would enforce the law on organizations and individuals not located in the PRC. 5) This article does not define data activities considered harmful to the PRC's national security, the public	We recommend removing the second paragraph of the article, and solely focusing on data activities in the PRC. For overseas threats to the PRC's national security we recommend existing laws and regulations be relied upon, such as the *National Security Law* and *Civil Code* to avoid unnecessary overlap and duplication

	according to the law**.**	interest or the lawful interest of citizens or organizations. It is therefore too broad to establish a baseline understanding of what should be done for compliance.	
3	"Data," as mentioned in this draft, refers to any record of information in electronic or non-electronic form. "Data activities" refers to data collection, storage, processing, use, provision, transaction, publication, and other such activities. "Data security" refers to the ability to ensure that data is effectively protected and lawfully used through adopting necessary measures and remains continually in a secure state.	The definitions of "data", "data security," and "data activities" are broad, vague, and can encompass all aspects of commercial activity. The *Cybersecurity Law* distinguishes data between personal information and important data. However, article 3 does not seem to contain this distinction, causing confusion on the Draft's alignment with the *Cybersecurity Law* and the proposed Personal Information Protection Law. The scope for the "provision" of data should not include data provided to affiliate, subsidiaries, or shareholders regardless of whether they are inside the People's Republic of China.	We suggest: The Draft should narrowly define and clarify the definition of key concepts such as "data," "data activities," "data security," "processing", "transaction" etc. It is essential to ensure the definition of these terms in relevant laws and regulations are consistent. Without such clarification, it will create significant challenges to corporate compliance as companies attempt to ensure the protection of data throughout its entire life cycle.

6	The Central national security leading body is responsible for policy decisions on and comprehensive coordination of data security work, researching, formulating, and guiding the implementation of national data security strategies and related major policies and plans.	It is unclear which government authorities are referred to in these articles, particularly what the “Central national security leading body” refers to.	The central and national security leading groups should be explicitly defined, and it should be clear whether the decision-making process will be managed at central level or decentralized to provincial/local level.

7	All localities and all departments bear primary responsibility for the data created, collected, or processed through the work of that locality or department as well as for data security. Supervising bodies are responsible for the supervision of data security in trades or sectors such as: industry; telecommunications; natural resources; hygiene and health; education; national defense science, technology, and industry; finance; etc. “Public security bodies and national security bodies are, according to the provisions of this Draft and relevant laws and administrative regulations, responsible for the supervision of data security within their respective scope of duties. The national cybersecurity and informatization department is, according to the provisions of	1) It is unclear which levels of government are being referred to by “all localities and all departments”, nor is it clear whether these departments have jurisdiction over data activities solely at their level or are also responsible for data activities carried out at subordinate levels. 2) There may be jurisdictional overlap between sector-specific administrative departments and public security organs, which can cause repetitive or redundant supervision.	We suggest the following: 1）Clarify the roles and responsibilities of the applicable national and regional bodies that will have authoritative oversight of data. Additionally, clarify how national and regional bodies will communicate guidelines and standards for these efforts. 2）Clarify boundaries between sector-specific administrative departments and public security organs to avoid conflicting enforcement and supervision.

	this Draft and relevant laws and administrative regulations, responsible for the comprehensive coordination of online data security and related supervision work."		

8	When conducting data activities, laws and administrative regulations must be observed, social public morals and ethics respected, commercial ethics observed, sincerity and trustworthiness upheld, data security protection duties fulfilled, and social responsibilities undertaken. It is prohibited to harm national security or the public interest, and it is prohibited to harm the lawful rights and interests of citizens and organizations.	Article 8 provides high level principles which are hard to objectively assess. Such broad principles will cause compliance challenges and may lead to inconsistent enforcement across different jurisdictions. Therefore, the Draft should provide specific guidelines.	We suggest revising the article for consistency with article 25 of the Draft which provides measurable standards.

10	The State actively engages in international exchange and cooperation in the data area, participates in the formulation of international regulation and standard-setting related to data security, and promotes the secure and free flow of data across borders.		It is encouraging that the Draft promotes international collaboration and exchange for data-related matters, standards setting, and promotes the free flow of data. We believe that interoperability with existing international frameworks and mechanisms should be a priority for China's development of cross-border data flow and security standards and regulations. We also encourage adding specific terms to ensure equal participation for multinational companies in the standard setting process, as per China's *Foreign Investment Law*.

11	Any organization or individual has the right to file a complaint about or report acts violating the provisions of this Draft to the relevant competent department. Departments receiving complaints or reports shall handle them promptly and according to the law.		In order to effectively file a complaint or report, “relevant competent departments” as referred to in this article must be clearly identified. In addition, the article should provide a timeline and further guidance regarding the procedure of filing and responding to complaints.

Chapter II	Data Security and Development		.
15	The State advances the construction of data development and use technology and data security standards systems. The State Council administrative department for standardization and relevant State Council departments will, according to their respective duties and responsibilities, organize the formulation and timely revision of standards concerning data development and use technologies and products and security-related standards. The State supports enterprises, research institutions, institutions of higher education, related sectoral organizations, etc., to participate in the formulation of standards.	We generally agree that standards setting is beneficial for the domestic market. However, we would like to note that standards should allow for the flexibility needed for companies to address sector-specific needs. Additionally, our members noted myriad requirements stemming from national or industry recommended standards referenced by laws and regulations lacking implementation details.	1) Standards regulations should be risk based and allow organizations to implement security measures based on their operating needs. 2) Data security standards should recognize and adopt international standards to the fullest extent possible and align as much as possible where full adoption is not feasible. 3) The Draft should specifically stipulate that mandatory requirements be clearly laid out in laws and regulations, and that companies cannot be forced to adopt recommended standards through direct reference by other laws and regulations.

16	The State promotes the development of services such as data security monitoring and assessment, certification, etc., and it supports specialized bodies for data security monitoring and assessment, certification, etc., to develop services according to law.		We recommend the following: 1) The article should contain assurances that foreign invested companies will be treated equally, and contain provisions allowing for self-assessment and certification. 2) A clear list should be provided of specialized bodies authorized to conduct data security assessments and certifications.

17	Network operators shall, when collecting important data or personal sensitive information for the purpose of business operations, specify the person responsible for data security. The person responsible for the data security shall be selected from among personnel who have relevant management work experience and professional knowledge on data protection, participate in important decisions of relevant data activities, and report work directly to the main responsible person of the network operators.	It is unclear what the precedent is for a unified data transaction market, and if there will be specialized laws and regulations to govern the data trading process as well the responsibilities and obligations of data traders.	We recommend formulating specialized laws and regulations to provide clarity and regulations for the “data transaction market” including trading entities, content, and data security, etc.
Chapter III	Data Security Systems		

19	The State shall implement data protection for data at different grades and classifications, according to the degree of importance to economic and social development; and according to the impact on national security, the public interest, or the lawful rights and interests of citizens or organizations if it is falsified, destroyed, leaked or illegally acquired, or illegally used. Each region and department, according to relevant national provisions, shall determine a regional, departmental, and industrial important data protection catalog, and undertake special protections for that which is listed in the catalog.	1) Members are concerned that provincial and departmental important data catalogs will not be consistent across geographical jurisdictions nor align with existing important data provisions in the *Cybersecurity Law*. 2) The decentralization and delegation of authority to local governments to define their own protection catalogues for "important data" may cause confusion with compliance requirements and present barriers to the free flow of data across China's jurisdictions. 3) There are insufficient details to determine who has the authority or what criteria will be used to determine scope of important data. At present it appears that regional government authorities will have broad interpretive powers for "important data." 4) What is the relationship between the State's grading and classification system for data and the development of important data catalogues by	We suggest the following: 1) The criteria and catalogue development process for important data" should be clarified, with development standards being consistent across all regions. All standards should provide a comment period for foreign companies to provide input. 2) The power to define the scope of and definition of important data should be limited and centralized at the industry level. 3) Clarify whether standard for data grading and classification will align with existing industry/national standards such as *Guidelines for Grading and Classifying Industrial Data (trial implementation), Guidance on Grading and Classification of Data in Securities and Futures Industry (JR/T 0158-208), Guidance on Grading of financial data security (draft for approval)* etc. 4) Clarify how types of data prevalent in multiple industries will be catalogued and classified.

		regions and departments? 6) In light of the variety of data used by various businesses, it is not apparent that a classification and hierarchy system with important data catalogues is feasible. 7) Important data as defined by the draft Data Security Management Measures does not include personal information or corporate data related to production, operation, and internal management. Will the Draft expand this scope?	
21	The State establishes a data security emergency management mechanism. In the event of a data security incident, the relevant department shall, according to law, activate a contingency plan, adopt appropriate emergency management measures, eliminate security gaps, prevent expansion of harms, and promptly publish to	It is unclear if this provision determines steps to be taken by the State in the event of a data security incident at the state/government level or whether this is intended to apply to data security incidents generally. The Draft does not clearly define a “data security incident” and is ambiguous on reporting times, which would impact companies’ obligation to report relevant incidents.	We propose the following suggestions: 1) The definition and scope of a “data security incident, “should be clarified. 2) Data controllers should report data breaches within 72 hours of awareness in line with the international standards, such as GDPR.

	society warning information relevant to the public.		

22	The State establishes a data security review system, where data activities that affect or may affect national security undergo national security review. Security review decisions issued according to law are final decisions	1) Key details of the data security review system need to be established, including the data security review process, which authorities can initiate a review, review timelines, etc. 2) It is unclear what guidelines or standards will be used to determine which data activities will be considered to have an impact on “national security.” Additionally, the wide-ranging definition of data activities increases the possibility that the security review will be broadly interpreted and applied beyond its intended scope. 3) Government involvement in commercial data activities should be limited to only what is necessary and data that can have an impact on national security at the highest level	We suggest the following: 1) Limit data security reviews only to important data that has been properly catalogued and classified at the highest protection level. 2) Provide a mechanism to dispute national security review outcomes and escalate to relevant national ministries. 3) Clarify how data security reviews will align with cybersecurity reviews to avoid overlap. 4) Provide clear guidelines on how a review is initiated, which data activities harm national security, who are the relevant reviewing authorities, and specifics on review mechanisms.

23	The State implements export controls according to law on data belonging to controlled categories to carry out international duties and safeguard national security.	The definition and scope of controlled categories remains unclear.	We suggest the following: 1) Specify which data belongs to export control categories and what specific measures are there for data export control. Similar to export control in the field of trade, the data related to the performance of international obligations and the maintenance of national security, would be classified as controlled items, and hence need to be licensed before export. 2) Clarify how this article will align with the draft Measures for the Security Assessment of Cross-Border Transmission of Personal Information.

24	For any country or region that adopts discriminatory prohibitions, limitations or other such measures toward the People's Republic of China with respect to investment or trade related to data, data development and use, or technology, the People's Republic of China may, according to the actual circumstances, adopt corresponding measures toward that country or region.	It is unclear what retaliatory measures may be taken against foreign governments who target China with discriminatory prohibitions. This may lead to retaliatory measures affecting foreign companies.	We recommend removing this article and addressing this article under more appropriate regulations such as the *Export Control Law.*
25	Those conducting data activities shall, according to the provisions of laws and administrative regulations as well as mandatory requirements in national standards, establish and complete a data security management system across the entire workflow, organize and conduct data security education and training, and		We recommend clarifying the requisite qualifications for data security personnel, and whether this role can be shared across parent companies and subsidiaries within China.

	adopt corresponding technical measures and other necessary measures to ensure data security. Those handling important data shall establish responsible data security personnel, and management bodies shall be established, to implement data security protection responsibilities.		
Chapter IV	Data Security Protection Responsibilities		

28	Those handling important data shall, according to regulations, periodically conduct risk assessments of their data activities, and submit a risk assessment report to the relevant competent department. The risk assessment report shall include: the categories and quantities of important data controlled by said organization; how data is collected, stored, processed, and used; the data security risks faced and countermeasures; etc.		We suggest the following: 1) Provide clear definitions on important data and important data operators. 2) Limit important data security assessments to only clearly identified data at the highest of level classification. 3) Limit the scope of activities that require risk assessment to important data processing activities as opposed to subjects who may possess important data.

29	Any organization or individual collecting data must adopt lawful and proper methods; they may not steal data or obtain it by other illegal means. Where laws and administrative regulations contain provisions on the purpose or scope of data collection or use, data shall be collected and used for the purpose and within the scope prescribed by laws and administrative regulations, and may not exceed the limits of necessity.	1) What does the term “proper methods” mean in this article?	We suggest deleting the term “proper method” from the article. The term “lawful method” is considered sufficient to express the intent of this article.

30	Bodies engaging in data transaction intermediary services shall, when providing trading intermediary services, require that the data providing party explain the source of the data, examine and verify the identity of both sides, and retain examination, verification, and transaction records	1) It is unclear what actions need to be taken by the data provider to “explain the source of the data.” It is unclear whether intermediary services are also required to verify the sources of data in a transaction.	We recommend clarifying the qualifications, authority, definition, etc. for a data transaction intermediary service body.

31	Operators providing specialized online data handling and other such services shall obtain a business license or register according to the law. Specific rules will be formulated by the State Council competent department for telecommunications jointly with relevant departments.	The relationship between this article's "online data handling" services and B21 definition of online data handling services in the 2015 Telecommunications Services Catalogue ("catalogue") is unclear.	We recommend that a clear definition be provided for online data handling services and how it aligns with the definition in the 2015 Telecommunications Services Catalogue ("catalogue")

32	Where public security departments and national departments need to consult data in order to lawfully safeguard national security or investigate a crime, they shall, according to relevant State regulations, undergo strict approval procedures and proceed according to the law; relevant organizations and individuals shall grant cooperation.	1) It is unclear what the procedures being referred to in this article are. 2) In practice there are often cases in which the competent authorities request confidential data from companies. However, some authorities do not provide written notifications, and instead only provide verbal notification. This forces companies into a dilemma where they must illegally provide data to an authority or suffer the consequences of non-compliance.	We propose the following suggestions: 1) Provide an appendix or table or publicly accessible website that identifies the national, regional, state, and industry regulators empowered by article 32 along with a point of contact. 2) Provide clarification on the scope and limits of requests for data by regulators from companies. Clarification should include protections for the legitimate interests of organizations and individuals. 3) Add articles regarding data security obligations of state organs.

33	Where foreign law enforcement bodies need to consult data stored within the mainland territory of the People's Republic of China, relevant organizations and individuals shall report the matter to the relevant competent department, and may only provide it after having obtained permission. Where the People's Republic of China has concluded or joined an international treaty or agreement with provisions on foreign law enforcement bodies consulting domestic data, those provisions shall be followed	The definition and scope of foreign law enforcement bodies is unclear, such as whether it includes overseas judicial agencies, tax bureaus, securities exchanges, clearing houses, etc. What is the scope of data that can only be provided upon approval from regulators? Who are the relevant competent departments in these cases? What if there is jurisdictional overlap?	We recommend the following: 1) Clarify the scope "foreign law enforcement bodies" and provide clarification on the type of data will require national, regional, or sector review 2) Limit the scope of data that can be provided to law enforcement upon request. 3) Provide more detailed regulations on the procedure, decisions making, and timeline of competent authorities.
Chapter VI	Legal Liability		

46	If government employees with the responsibility of overseeing data security neglect their duty, abuse their power, or abuse their position for private gain, yet it does not constitute a crime, they shall be sanctioned in accordance with the law.	Does “government employee” as in this article refer to government staff specifically responsible for data security or staff that will supervise all organization and individuals? If it’s the latter, it will be necessary to add an article for the protection of trade secrets and proprietary information and also provide civil compensation on top of criminal liabilities if any such infringement upon trade secrets or proprietary information occurs and causes losses to business.	We suggest revising this article to: “If government employees with the responsibility of overseeing data security neglect their duty, abuse their power, infringe trade secrets or other proprietary information, or abuse their position for private gain, yet it does not constitute a crime, they shall be sanctioned in accordance with the law and liable for civil compensation for infringements of trade secrets and proprietary information.”
47	Using data activities to harm national security or the public interest, or to harm the lawful rights and interests of citizens or organizations, shall be punished according to relevant provisions of law and administrative regulations.	See comments on article 3	Remove the provision.