# US-China Business Council Comments on The Draft Administrative Measures on the Security Assessment of the Overseas Transfer of Personal Information and Important Data

*May 11, 2017*

On behalf of the 200 members of the US-China Business Council (USCBC), we appreciate the opportunity to provide comments to the Cybersecurity Administration of China (CAC) on the Draft Administrative Measures on the Security Assessment of the Overseas Transfer of Personal Information and Important Data (the "draft measures"). Our member companies represent a wide variety of manufacturing and service industries, all of which operate and use information networks. These diverse members are united in their commitment to promoting and participating in an open and healthy commercial environment that supports China's development and the use of big data as a driver of economic growth.

The free flow of data across borders is an essential part of an innovative digital economy, the development of which China has made a priority. Chinese initiatives like the 13th Five-Year Plan, Made in China 2025, and Internet+ emphasize the development of smart- and internet-based technology. Speeches by senior officials regularly emphasize the importance of an open and interconnected internet both within China and under the G20 framework. These efforts can be strengthened by using the best practices and expertise offered by international companies, which have experience integrating business practices with global information networks. Allowing companies and interactive products to access information around the world is a key component of "smart technology— a goal of the 13th Five-Year Plan — and is necessary for successful high-level policy plans across sectors, such as Internet+, the Big Data Promotion Plan, and development plans for greater energy efficiency via smart cities or China's financial industry.

Seventy-nine percent of USCBC members cited concerns about China's approach to information flows and technology security in USCBC's 2016 member survey, largely due to the negative impacts those policies have on companies' ability to conduct normal business operations. As written, the draft measures will impact the operations of companies — both foreign and domestic — in ways unseen in other markets.

To address these concerns, USCBC recommends clarifying some articles in the draft measures. We also note that certain obligations imposed on companies and government agencies may hinder the goals outlined in the draft measures. Addressing these concerns in a comprehensive manner by consulting with industry will enhance China's data security by ensuring companies can leverage big data solutions to support China's economic development.

**Article 2:**

Our members are concerned that Article 2 greatly expands the scope and scale of data localization requirements beyond existing regulations such as the Cybersecurity Law. Article 2 requires that personal information and important data gathered or produced by network operators during operations in China be stored within the country. However, under Article 37 of the Cybersecurity Law, only personal information and important data collected by critical information infrastructure (CII) operators is required to be localized. The expansion from "CII" to "network operator" greatly broadens the scope of data that would qualify for localization, creating inconsistency and potential confusion for companies seeking to comply with China's laws. It also may impose unreasonable and additional workloads on industry stakeholders that need to frequently share data with their business partners, parent companies, and affiliated companies overseas. Additionally, the current definition of "important data" is overly broad, making it difficult for companies to fully comply with the requirements of the draft measures.
We recommend CAC align the scope of the draft measures with the scope stated in the Article 37 of the Cybersecurity Law, requiring only personal data collected by CII operators to undergo data security review. We also recommend that the general rule apply only to personal data, eliminating "important data" from the scope of the draft measures.

**Article 4:**

Language in Article 4 requiring industry stakeholders to affirm consent from data subjects in every circumstance is extremely onerous and goes beyond existing consent collection practices by industry regulators. Data subjects are implicitly aware that their information might be utilized when they participate in ecommerce markets, subscribe to financial services, or generally engage in online activity. For example, when a Chinese consumer submits credit card payment information to conduct a cross-border transaction with an overseas seller, the consumer implicitly understands that necessary payment information will cross borders for the payment to be processed. We recommend that "implied consent" be a sufficient standard for proceeding with outbound data transfer.

Additionally, as noted above, by expanding the scope from CII to network operators, the draft measures impose heavy personal information disclosure obligations compared to the Cybersecurity Law. Although network operators do collect information, in practice they are not typically the parties best positioned to anticipate the transfer of specific personal information out of China or to notify individuals of outbound transfers in advance. Thus, we recommend that some exceptions to the obligations for transferring personal information out of China be added to Article 4 and that any data collected before the implementation of the draft measures be exempted from future data security review requirements.
As an example, in the financial services industry, there are two types of personal information a financial institution collects: personal information relating to employees of the institution, and personal information relating to clients, such as the personal information of a corporate client's directors, legal representatives and authorized signatories. It is unclear if Article 4 will apply to the first, second, or both types of information. Currently, China's financial regulators—including the People's Bank of China, China Banking Regulatory Commission, and China Securities Regulatory Commission—require financial institutions to collect certain individuals' personal information for "Know Your Customer" requirements and other purposes. A financial firm usually relies on its corporate clients to obtain the consent from relevant individuals to enable the firm to disclose or process personal data. It is unrealistic for financial institutions to obtain such individual consent directly.

We recommend CAC clarify if personal information would apply to employees or clients or both. We further recommend that CAC take into consideration existing consent collection practices across industry regulators and ensure the draft measures align with the regulations issued by those regulators.

**Article 5:**

Article 5 is insufficiently clear about whether CAC's role is limited to coordination and guidance or if its authority extends to overruling the assessment decisions made by relevant industry departments and regulatory authorities. We recommend CAC clarify if the relationships and respective responsibilities of competent industry departments, regulatory authorities, and CAC are hierarchical, and how it will process review appeals.

**Article 6:**

Article 6 offers broad authority to supervisory groups to interpret implementation of the data security review. This authority will likely lead to divergent, and possibly contradictory, enforcement processes. Insufficient transparency and inconsistent interpretation between and within government agencies can foster uncertainty and ambiguity for companies operating in China. Without clear guidance, authorities will misinterpret information, forms, and materials that are required for the data security review process, leading to radically different review processes by regulatory agencies. This will unnecessarily complicate the data review process, and cause confusion among companies seeking to invest in China. We recommend aligning data security review processes across agencies to ensure unified implementation.

**Article 7:**

Article 7 calls for network operators to conduct a data security self-assessment before transferring data overseas, however the mechanism and liability for self-assessment remain unclear. We recommend CAC recognize the APEC Cross Border Privacy Rules (CBPR) system as a mechanism to confirm that privacy rights are respected. We also recommend that compliance with the APEC CBPR system be recognized as a basis for transfer of data out of China as required under the draft measures. If that is unacceptable, we recommend CAC clarify the number of security assessments a network operator is subject to and the specific types (e.g. self-assessment, assessment by regulatory authorities), to ensure clarity and identify areas where duplicative reviews may be occurring. In some cases, such as in the financial services industry, a company may be under the authority of multiple industry regulators. We recommend clarifying which agencies have what level of jurisdiction in cases where industries are overseen by multiple regulators, and we recommend limiting duplicative security review processes to eliminate unnecessary administrative burdens on industry stakeholders.

Finally, we recommend all enterprise internal data transfers be excluded from the security review process to facilitate MNCs—both Chinese and foreign-parented—doing business worldwide.

**Article 8:**

Though Article 8 defines the assessment criteria for data transfer, it does not specify the situations in which transfers are prohibited or the procedures for assessment of proposed transfers. This essentially isolates foreign multinational companies from their parent organizations by forcing an industry stakeholder to justify--without clear regulatory requirements--that a country or region is sufficiently secure to protect transferred data. This goes far beyond the capabilities of industry. We recommend that subsection 4 be removed entirely, as it is not related to protecting personal information or important data.

**Article 9:**

Article 9 is insufficiently clear for companies to implement appropriate safeguards. We recommend adding language indicating that the approach to security assessment will "promote network information in

accordance with the free flow of information ." The following changes will ensure smooth industry implementation:

- Subsections 1 and 2 specify the amount of data without indicating if the amount is based on individual transfers or total transfers over time. We recommend CAC remove the criteria on data exceeding 1,000 GB and containing the personal information of more than 500,000 individuals, as these thresholds are arbitrary and will pose a significant burden for CAC, industry regulators conducting security reviews, and industry stakeholders that will rapidly reach the limits imposed by the draft measures. We further recommend that assessment criteria focus on the nature of the data, as opposed to data volume.

- Subsection 3 is not clear on what is information on chemistry and biology or information on population health. The scope should be limited only to such information that may trigger national security concerns such as information relevant to the development of biochemical weapons for example. Otherwise, the existing language could be broadly interpreted to contain information on the development of chemical or biologic medicines and patient information collected through clinical trials conducted for the registration of such products. If such information would fall under the scope, it will add significant burden to the healthcare industry's--both foreign and domestic)--R&D activities in China which require cross border transfer of research data in the context of global research activities, undermining China's goals to become a more innovative society.

- Subsection 6 authorizes relevant industry regulators to determine if the outbound transfer of data may influence national security and social public interests. This language offers industry regulators sole discretion to restrict data transfer, undermining the rule of law. We recommend adding the following language to Subsection 6 "relevant regulatory authorities are entitled to decide, subject to any other laws and regulations".

Finally, we recommend CAC clearly articulate the process through which the organization under review can appeal a negative review result.

**Article 10:**

Though we appreciate the effort to limit the timeframe for statutory security reviews, the draft timeframe of 60 working days is too long. A delay of that length would be enormously disruptive for industry stakeholders' regular business operations. We recommend normal data transfers be allowed to continue throughout the security review process, to limit business disruption.

**Article 11:**

While we understand the interest in prohibiting data transfers to limit risks to national security, the stipulations laid out in Article 11 are vague, high-level, and difficult for industry stakeholders to comply with. We recommend the following changes:

- Subsection 1 requires industry stakeholders to affirm consent from data subjects in every circumstance. This is extremely onerous and goes beyond existing consent collection practices by industry regulators. We recommend that implied consent be a sufficient standard for proceeding with outbound data transfer.

- The risks enumerated in Subsection 2 should be narrowed. We recommend limiting the clause to "The cross-border data transfer poses risks likely to affect the national security of China."

- Subsection 3 offers complete authority for any industry regulator to impose data localization under any circumstance it determines necessary. We recommend changing, "Other circumstances in which the national cyberspace, public security, security, or other relevant departments determine that the data concerned is prohibited from being transferred overseas." to read "Other circumstances in which the national cyberspace, public security, security, or other relevant departments, in accordance with relevant specific laws and regulations, determine that the data concerned is prohibited from being transferred overseas."

**Article 12:**

Requiring a mandatory yearly data export audit will significantly increase the administrative burden on industry stakeholders. We recommend that mandatory reviews occur once every three years to ease the administrative burden.

In addition, the requirement to undergo a new security review in case of "significant changes" to the recipient of data is very broad. We recommend clarifying what constitutes a significant change. We also recommend adding language to clarify that "Article 12 only applies in cases where thresholds for Article 9 are met."

We suggest rewording the article to ensure a reasonable period of remediation can occur in advance of reporting to relevant regulators.

Finally, USCBC encourages CAC to publish a data export report template to assist industry stakeholders with the filing process.

**Article 16:**

Article 16 is very broad, and appears to apply to any industry stakeholder transferring data, we recommend this article be deleted.

**Article 17:**

As mentioned in our comments on Article 2, the current definition of "important data" is overly broad, making it difficult for companies to fully comply with the requirements of the draft measures. We recommend deleting "important data" throughout the draft measures. If that is unacceptable, we alternatively suggest CAC provide specific examples of what constitutes "important data" to ensure effective company compliance.

Additionally, the definition of "cross-border data transfer" is also overly broad. Under the current Internet and network technology, to "provide overseas institutions, organizations, or individuals with personal information and important data" can be achieved by dozens of different means, either online or offline, actively or negatively. For example, if an industry stakeholder does not provide encryption or access-rights control on personal data stored in its intranet, we are concerned this will be deemed as violation of "Cross-border data transfer" prohibition by regulator. As noted in Article 7 above, we recommend all enterprise internal data transfers be excluded from the security review process to facilitate MNCs—both Chinese and foreign-parented—doing business worldwide.

**Article 18:**

It is premature to set an implementation date in 2017 without thorough consultation with industry stakeholders, faithful review of submitted comments, and multiple rounds of revision. We recommend delaying implementation of the regulations to ensure a thorough vetting with domestic and international industry stakeholders. We also recommend at the time of implementation, a one-year grace period be imposed to ensure industry has sufficient time to adjust internal compliance processes to satisfy the requirements of the draft measures.