THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

US-China Business Council Comments on

The Draft Measures for Security Review of Online Products and Services

March 6, 2017

On behalf of the more than 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 Measures for Security Review of Online Products and Services (the Draft Measures)*. Our member companies represent a wide variety of industries, including companies that sell and purchase information security products and services, as well as companies that operate and use information networks. These diverse members are united in their commitment to promoting and participating in an open, healthy commercial environment that supports China's development and promotes the use of information technology as a driver of economic growth.

USCBC and our members recognize that the drafting of these measures reflects a desire by the Chinese government to promote information security and the lawful rights of Chinese citizens and organizations. Our companies share these goals, and have global expertise in working with governments and other industry players to achieve these objectives while promoting robust industry development. Many of our members have long offered high-quality information security products and services in China, contributing actively to the development of this industry.

We recognize the *Draft Measures* as part of a broader emerging legal framework that includes the *draft cybersecurity strategy*, *the Counterterror Law*, *the Cybersecurity Law*, and *the National Security Law*. USCBC encourages clarification of how the *Draft Measures* will relate to these measures, as well as other existing laws and regulations. These include, but are not limited to, *China's Criminal Law*, the development of *China's cybersecurity review regime*, and the existing MLPS framework that was promulgated by the Ministry of Public Security in 2007.

USCBC appreciates the opportunity to offer additional comments on the *Draft Measures*. We recommend clarification of some articles; we also note that certain obligations imposed on companies and government agencies may actually hinder the cybersecurity goals of the *Draft Measures*. Addressing these concerns in a comprehensive manner will ensure China's information security by encouraging companies to deploy the best and most secure technology available in China.

Article 1:

The *Draft Measure*s indicate network products or services are subject to a secure and controllable review. However, this article does not cross-reference key terms such as "key network products and services" with existing articles contained in the *National Security Law of the People's Republic of China* or the *Cybersecurity Law of the People's Republic of China*, nor does it define these terms. USCBC recommends that CAC define the extent and scope of "network products and services" to either confirm

that it is products and services provided by "network operators," as defined in the *Cybersecurity Law of the People's Republic of China*, or otherwise clarify the term if it does not align with this definition.

USCBC suggests narrowing the scope of network products by defining "network products" as "core communications infrastructure equipment including routers, switches, bridges and inter-network gateways." We also recommend explicitly stating that terminals and edge/access equipment are excluded from the definition of "network products."

Article 1 further notes that the cybersecurity review is based on "public interests," a term not included in the two laws cited above. Since there is no clear definition of "public interests" as they pertain to cybersecurity, this term is vulnerable to inconsistent interpretation and is likely to create confusion in enforcement and compliance with the law. We therefore suggest that the term "public interests" be deleted from the final version of the Measures.

Article 2:

Article 2 should clarify what online products and services are related to "National Security and Public Interests." Article 23 of the Cybersecurity Law defines similar products as "critical equipment for networks and dedicated products for cybersecurity." USCBC suggests the Draft Measures adopt the same terminology used in the Cybersecurity Law if the intention is to refer to the same set of products and services. Additionally, we suggest the definition of network products and services not include open source products used in information systems developed by financial and other institutions. These clarifications should also state that the review only applies to the network products and services, not the information systems using those products and services.

As noted in our comments on Article 1, we suggest that "public interests" be deleted from the final version of the Measures.

Article 3:

The Draft Measures indicate that network products & services and their suppliers are subject to the cybersecurity review. We recommend CAC recognize existing global best practices of utilizing relevant international standards and best practices to ensure suppliers maintain supply chain integrity. As such, we suggest replacing "their suppliers" with "supply chain."

We further suggest CAC either issue implementing guidelines or provide supplementary information detailing the cybersecurity review methodology. Aligning the cybersecurity review methodology to international standards would be a positive initiative and meet China's goal of aligning with international standards processes.

Article 4:

Article 4 details risks that trigger a cybersecurity review. However, as written these risks are overly vague and better addressed by existing review and enforcement mechanisms. For example:

- Article 4.3 indicates that user information is a national security concern; user information is best protected through the enforcement of existing regulations outside the scope of national security reviews, for example, *the Cybersecurity Law*.
- Article 4.4 states that products and services which can be used for unfair competition are subject to cybersecurity review. Competition challenges would be better addressed if existing regulations were enforced by the three competition enforcement regulators (NDRC, AIC, MOFCOM).
- Article 4.5 covers "other risks that may endanger national security and public interest." This is overly broad and could potentially cover all products and services in the market.

USCBC suggests that section 3, 4, and 5 be deleted. Or, to make clarification of how the *Draft Measures* will relate to other existing laws and regulations.

Article 6:

The Draft Measures currently offer no prohibition of potential conflicts of interest or explicit protections of intellectual property submitted through the expert review process. CAC should consider additional steps to ensure trade secret information is protected during expert panel reviews and that competitors are not named as experts on review panels. To do this, USCBC recommends that additional language be added to the Draft Measures, based on the following principles:

- **Prevent individuals with a conflict of interest in a review from serving on an expert panel**. CAC should also establish rules prohibiting the naming of experts with clear conflicts of interest to applicants' expert panels and requiring those with a conflict of interest be removed.
- **Institute a formal process for applicants to dispute expert panel nominations where conflicts of interest exist**. This process should include a public timeline for consideration, review, and resolution of the dispute to minimize disruptions in the investment process.
- **Ensure that applicants can provide input on expert panel nominations**. CAC should provide updated and complete lists of approved experts to companies and allow them to nominate a certain number of experts to the panel.
- **Institute clear guidelines for requests involving sensitive company information**. CAC should require experts to support information requests with substantiated facts, commercial experience, and sound science. Clear and formal processes should be created to manage such requests, including a timeline in which requests must be made and for companies to respond.
- **Provide clear information about the rules governing certification, selection, use, and operating conduct of expert panels.** This information should be distributed to officials, industry, and the public via implementing measures, public seminars, or other means. It should also include obligations for experts to withdraw from a case based on a conflict of interest.

Article 6 further stipulates that the "trustworthiness" of suppliers is a factor in the cybersecurity review. Without a definition, the term is difficult to evaluate. We suggest replacing "and the security and trustworthiness of the suppliers" with "including the use of relevant international standards to address supply chain risks."

Article 8:

Article 8 notes that both "national industry associations and the voices of market entities" can trigger cybersecurity reviews. USCBC is concerned that these terms are overly broad and might be abused by some enterprises to achieve an unfair competitive advantage. We suggest deleting "or any national industry association, or based on the voices of market entities" to limit these competitive concerns.

USCBC further recommends that CAC clearly articulate the process through which the organization under review can appeal a negative review result.

Article 8 also stipulates that the results of the cybersecurity review will be made public. USCBC suggests that all information available publicly be approved by the organization under review and only general product and service information which does not contain information that might be considered trade secrets be made public.

Article 9:

Article 9 defines "key sectors" subject to the cybersecurity review by relevant ministries, but the sectors specified differ from the industry sectors defined as "Critical Information Infrastructure" under Article 31 of the China Cybersecurity Law. USCBC suggests CAC align the "key sectors" with the industry sectors defined as "Critical Information Infrastructure" under Article 31 of the China Cybersecurity Law for consistency and to avoid potential confusion.

Article 10:

Article 10 indicates that government departments and key sectors will give priority to products which have passed the cyber security review. We recommend that CAC define the meaning of "give priority," and limit this requirement to only Critical Information Infrastructure as defined under the China Cyber Security Law rather than all companies in those sectors. We further suggest this requirement apply only to the purchase of new equipment.

Article 11:

Article 11 indicates that any product or service procured by the operators of critical information infrastructure (CII) should undergo cybersecurity review. The Draft Measures cover a broad range of CII while simultaneously leaving the specific scope to be determined by other regulations. We suggest CII be fully defined and a list of all industries considered CII be published for public comment. We also suggest that regulators further clarify "the departments in charge of CII protection," particularly for cross-sector network products.

Article 13:

Article 13 requires third party institutions and other relevant units and personnel have an obligation to keep any information obtained from the security review secure and secret, and are not permitted to use this information for purposes outside of the cybersecurity review. We further recommend that expert panelists should be required to return or destroy all data collected during their work on an expert panel. Regulations should outline specific consequences when such provisions are violated.

CONCLUSION

USCBC thanks the Cybersecurity Administration of China for providing this opportunity to comment on the draft regulations. We hope that these comments are constructive and useful to the Cybersecurity Administration of China as it reviews the *draft measures*. We would appreciate the opportunity for further dialogue on these issues and are happy to follow up as appropriate.

—END—

The US-China Business Council

Contact: Jake Parker, Vice President, China Operations

Tel: 010-6592-0727

Fax: 010-6512-5854

E-mail: jparker@uschina.org.cn