WORLD TRADE ORGANIZATION

S/C/W/378

5 October 2018

(18-6169)

Page: 1/3

Council for Trade in Services

Original: English

COMMUNICATION FROM THE UNITED STATES

MEASURES ADOPTED AND UNDER DEVELOPMENT BY CHINA RELATING TO ITS CYBERSECURITY LAW

Questions to China

The following communication, dated 3 October 2018, from the delegation of the United States is being circulated to the Members of the Council for Trade in Services.

Over the past two years, WTO Members, the international business community and other stakeholders have raised serious concerns regarding China's Cybersecurity Law and various draft implementing measures connected with the Cybersecurity Law (and in some cases China's National Security Law). Among other things, these concerns relate to elements of those draft implementing measures that would restrict cross-border transfers of information and that would require the localization of data in China.

The United States has submitted two previous communications to the Council for Trade in Services relating to China's Cybersecurity Law. On 26 September 2017, the United States submitted a communication to the Council on "Measures Adopted and Other Development by China Relating to its Cybersecurity Law" (S/C/W/374), which focused on the issues of cross-border transfers of information and data localization. On 23 February 2018, the United States submitted a follow-up communication that included this same topic (S/C/W/376).

In its prior communications, the United States alerted Members to two key draft implementing measures in this area, i.e., the "Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data" and the "National Standard — Information Security Technology — Guidelines for Data Cross-Border Transfer Security Assessment." With regard to these draft implementing measures, various stakeholders have expressed strong concerns about China's proposed approach to require a burdensome security assessment for transfers of any data Chinese government officials consider to be "important data" These stakeholders also have objected to China's proposed approach to require such a burdensome security assessment for the transfer of personal information, which would, in virtually all circumstances, require explicit consent by the owner of the information before any cross-border transfer can take place. China also has proposed that any "important data" or "personal information" that operators of critical information infrastructure collect or generate in China must be stored in China. These aspects, taken together, could disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business.

1 QUESTIONS TO CHINA

1. At present, it remains unclear whether or how China will revise its proposed approach to take into account these concerns. Given the importance and seriousness of the issues raised by China's

developing cybersecurity regime, the United States poses the following lingering questions that it will be essential for China to answer:

a. How does China plan to proceed with revising the draft implementing measures cited above to respond to the concerns that have been articulated?

b. Does China intend to release additional new draft implementing measures? If so, can China confirm that it will provide reasonable advance notice and an opportunity for all stakeholders to comment on those new draft implementing measures?

c. Many stakeholders have expressed strong concerns about China's proposed restrictions on the undefined category of "important data." The draft implementing measures cited above define important data as "data closely related to national security, economic development and societal and public interests." While China has further explained that "the important data refers to importance for the nation, not for enterprises or individuals," the scope of this category, and how and by whom it would be defined, remain unclear. Who would decide what data is "important for the nation"? The enterprise? The Cyberspace Administration of China? A sector-specific regulator?

d. How is it possible to decide what data is "important data" in a manner that is not arbitrary?

e. The draft implementing measures cited above would apply to all network operators, broadly defined as "network owners, administrators and network services providers." Does this refer solely to a company that actually operates a network, such a telecommunications company? Does it also apply to a company that uses a network (which is, in practice, all companies)?

f. Elsewhere, China has stated that its draft implementing measures would apply specifically to operators of "critical information infrastructure" (CII), not to all network operators. Even if China were to limit its application of these measures to operators of CII, China's proposed definition and approach to CII would continue to raise serious concerns. In this regard, at least two of the draft standards that China released for public comment in June 2018 relate to CII, i.e., "Information Security Technology – Security Controls of Critical Information Infrastructure" and "Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure." The scope of what is identified as CII in these draft measures (as well as in China's Cybersecurity Law itself) continues to be broad and vague, extending well beyond traditional national definitions of CII, which could result in substantial barriers to foreign service suppliers inside and outside of China. Can China confirm that it intends to revise its approach and to narrow its definition of CII?

g. The draft measure entitled "Information Security Technology – Security Controls of Critical Information Infrastructure" includes a number of restrictive requirements for cross-border data flows:

- In virtually all circumstances, it continues to set forth "explicit consent" as the only basis for the CII operator to collect, use or further share the "personal information" of individuals;
- It provides that any "personal information" or "important data" that CII operators collect or generate through operations in China must be stored in China; and
- It provides that if the transfer of "personal information" or "important data" is required for business reasons, the CII operator would need to conduct a "security assessment" or would be subject to a state-implemented "security assessment" of the proposed transfer that appears quite burdensome.

h. Regarding "personal information" in particular, the United States has suggested that China provide other means for the CII operator to meet any requirements regarding the collection, use or sharing of this information, such as the APEC Cross-Border Privacy Rules System (CBPR). Can China confirm that it is considering the adoption of an alternative, less burdensome mechanism, such as the CBPR?

i. On 17 March 2018, China's "Measures for the Administration of Scientific Data" took effect. This measure includes basic rules for managing scientific data in China and would, inter alia, restrict cross-border transfers of this type of data. China did not publish this measure in draft for public comment. Will China agree to suspend implementation of this measure so that it can seek public comment on it and revise it as appropriate in light of the concerns raised by stakeholders?