June 1, 2016

Chairman Xiang Junbo
China Insurance Regulatory Commission
15 Jinrong Dajie, Xicheng Qu
Beijing 100140
People's Republic of China

Re: G/TBT/N/CHN/1172

Via WTO TBT Entry Point system

Dear Chairman Xiang:

The below associations have reviewed China's April 19, 2016 notification G/TBT/N/CHN/1172 to the Committee on Technical Barriers to Trade of the World Trade Organization on the Provisions on Insurance System Informatization (the "Provisions"). We appreciate that this has been submitted in accordance with China's commitments to the World Trade Organization (WTO) and China's recognition that the potential technical barriers to trade present in the Provisions warrant notification to the TBT Committee for comment. We also recognize that the China Insurance Regulatory Commission (CIRC) has made some changes from the original version released for comment domestically in the fall of 2015.

Unfortunately, the members of our associations believe that the current draft still does not address international industries' primary concerns and respectfully bring those strong concerns to your attention.

In addition, these concerns are amplified by the fact that the proposed date of adoption for the Provisions has been set for the day after the comment period ends, clearly suggesting that the regulators do not intend to make any modifications to the Provisions based on the comments that are submitted. The TBT Agreement requires WTO members to publish notices early enough for interested parties to review it, with sufficient time for comments taken into account in final measures. As a consequence, we ask that adoption of the Provisions be suspended to allow suitable time for further stakeholder input and consideration of the substantive concerns raised in this notification and in those of others, in line with TBT commitments.

China, like other WTO members, has the right to implement measures necessary for the maintenance of cybersecurity, but we believe that the Provisions go far beyond what is necessary. If adopted as currently drafted, however, the Provisions would create unnecessary obstacles to international trade and likely to constitute a means of arbitrary or unjustifiable discrimination against producers and service providers in countries where the same conditions prevail. As a consequence, we have concerns that the Provisions could constitute an unnecessary obstacle to international trade.

Based on these concerns, and those detailed below, we believe that the Provisions are in urgent need of substantial revision before adoption, and would ask that the adoption date be delayed to allow further stakeholder input and dialogue.

Of particular concern are the following provisions:

Data residency

Article 31, paragraph 2 of the Provisions requires that data originating within China be stored within China. This provision would impose a geographic restriction on data flows, increasing costs without increasing data security. Relevant insurance institutions bear responsibility for such data security and can be held liable by China's prudential supervisor for any material breach. In addition to not increasing security, this requirement also does not decrease the risk of data breaches from outside of China, as modern data storage and retrieval technology render the location of data centers immaterial.

This provision would, however, increase the operating costs of smaller insurers, in particular foreign-invested insurers which in aggregate have a market share in China of approximately 5 percent in life insurance and less than 2 percent in property insurance. As drafted, the data residency requirement would also apply to insurance institutions' service providers including accounting, advertising and law firms which, out of necessity, have access to such data.

In addition, any requirement to outsource data storage services within China's borders would limit the ability of international companies to effectively run their business as part of their global platforms, negatively impacting their operations and creating security risks. Local IT solutions may not be immediately or fully compatible with global information security regimes, which are often designed and maintained by company headquarters in their home markets. Using China-specific solutions that are out of sync with global security networks may create security vulnerabilities specifically for data that has been collected in China, and would work against the information security goals of this draft document.

Because of these concerns, we ask that Article 31 be removed.

Cross-Border Data Transfer

Article 58 of the Provisions requires that all international data transfers be conducted in accordance with relevant Chinese regulations, without specifying the content or identity of such regulations. Such vagueness could make compliance an impossibility and discourage cross-border data transfers, even though such transfers yield substantial efficiencies, particularly for global foreign insurance institutions which have need for centralized data analysis.

To ensure that these business functions operations remain uninterrupted, we ask that these provisions explicitly allow for copies of financial data to leave China's shores for business and analytical purposes. This would allow companies to optimize their services within the digital modern economy, while still preserving the jurisdiction of relevant Chinese authorities.

Information and Communications Technology (ICT)

Article 53 of the Provisions requires that insurance institutions give preference in the procurement of informatization products to those that are "secure and controllable." Our understanding is that the criteria for the determination of what constitutes "secure and controllable" have yet to be specified.

We are concerned, however, that as "secure and controllable" has previously been defined in other draft measures as ownership of domestically-owned and registered IP, this article will be interpreted to mean domestic production by domestically-invested and/or controlled producers. This would have a particularly adverse impact on global insurance institutions which would be required to procure potentially duplicative or incompatible hardware, software and services than their global networks currently use, thereby reducing their competitiveness. This issue is exacerbated by the fact that it would affect both commercial and public procurement.

Moreover, forcing companies to adopt hardware, software, or services that may be incompatible with or otherwise inferior to their global IT management standards may negatively impact their global information security regimes. If multinational companies are forced to create separate IT solutions for products that are specific to China, then they will be prevented from applying their global information security practices in the market. For example, if data leakage or data theft occurs on a system isolated to a China-based network, and global monitoring systems are unable to pick up on this incident due to network incompatibility between China-based and global systems, then the company's response in terms of speed, containment, or customer alerts may be compromised. These risks work against the overall goals of this document in terms of enhancing IT security.

Our concern on "secure and controllable" is heightened by public remarks by officials with responsibility for information technology in the financial sector linking "secure and controllable" to industrial policy goals of promoting domestic products and services, even at the cost of accepting lower quality and security defects – a stance which is inherently inconsistent with the Provisions' goal to increase information security and with previous statements made bilaterally at the State Leader level, by which Chinese officials guaranteed that "secure and controllable" policies would not discriminate against foreign products.

We recommend that any requirement to use secure and controllable technology be removed from the provisions until the definition of the term includes technical specifications or minimum security standards based on international standards and does not discriminate against foreign IT. This definition should make clear that secure and controllable requirements will not mandate or preference the procurement or use of Chinese-origin products, technologies, intellectual property, or standards. All companies – in insurance and other sectors – should be allowed to determine the types of information products that bests fits their own security needs.

Cryptography

Article 54 of the Provisions requires that cryptography in insurance institutions meet Chinese national requirements. While this is a change from previous versions of the regulation, this article would presumably require cryptography to comply with the January 2014 National Work Plan for Promoting Application of Cryptography in the Financial Sector and the 2015 Insurance Industry Cryptographic Application Implementation Plan, which called for the complete adoption of Chinese domestic cryptographic standards and related specifications by 2020 for any and all products such as internet browsers, PCs, laptops, mobile phones, and servers.

This mandate would impose a disproportionate burden on foreign-invested insurers, which would have to implement Chinese algorithms that may differ from those used by their parent

companies. Implementing unique cryptopgraphy for a single country in a global network will increase the risks that an insurance company's systems could be illegally infiltrated – a circumstance that international insurers and regulators constantly seek to minimize.

Furthermore, these regulations are contrary to the encryption commitments the Chinese government made at the World Semiconductor Council (WSC) Government and Authorities Meeting on Semiconductors (GAMS) in 2010, as as they reflect direct intervention into commercial mass market encryption products. The uncertainty over whether local encryption standards are consistent with international standards also raises security concerns. International best practice is that firms use international encryption standards to minimize problems across systems in different countries and ensure that client data is as well protected as possible – something that industry regulations require as well.

We recommend the Provisions remove the requirement for cryptography to meet Chinese national requirements and instead allow the use of international encryption standards.

Multi-Level Protection Scheme

Article 56 of the Provisions sets information system security requirements in accordance with the Multi-Level Protection Scheme (MLPS) without specifying the linkage between specific insurance industry information systems and national security.

We are concerned that information systems with no direct bearing on national security may be assessed at Level 3 or higher, yet we are aware that Article 21 of the Administrative Regulations for the Hierarchical Protection of Information Security establishes a preference for domestically-invested or controlled information security products with Chinese core technology. This would disproportionately impact foreign-invested insurance institutions whose operations outside China would be under no such obligation and would unnecessarily discriminate against foreign IT providers.

We recommend that Article 56 be removed from the Provisions.

Information System Security Certification

Article 57 of the Provisions requires that insurance systems with a need for certification of their information security management systems engage an institution approved by the State certification and accreditation supervision and administration authority. We are concerned that such a restriction on the choice of certification institutions would bar insurers from engaging foreign certification institutions. International standards such as the ISO/IEC 27000 family of standards on information security management are clearly applicable to the Provisions' goals, and thousands of organizations (and many governments) already rely on these standards today to ensure the security of their information assets.

We recommend that Article 57 be revised to reference international standards as the most effective and appropriate way ensure data security.

Conclusion

We thank you for your consideration of our concerns. We ask that adoption of the Provisions be postponed to allow further stakeholder input and to ensure that appropriate security regulations can be instituted in such a way as to advance China's legitimate security interests, while avoiding commercial interruptions or international disputes.

We look forward to further discussion regarding these issues.

Sincerely,

American Chamber of Commerce in China
American Chamber of Commerce in Shanghai
American Chamber of Commerce in South China
American Council of Life Insurers (ACLI)
American Insurance Association (AIA)
Asia Securities Industry & Financial Markets Association (ASIFMA)
BSA | The Software Alliance (BSA)
Canada-China Business Council
Coalition of Services Industries
Communications and Information Network Association of Japan (CIAJ)
Digital Europe
European Services Forum
Financial Services Forum
Information Technology Industry Association (ITI)
Japan Business Machine and Information System Industries Association (JBMIA)
Japan Electronics and Information Technology Industries Association (JEITA)
The Japanese Chamber of Commerce and Industry in China (JCCIC)
National Foreign Trade Council
PCI Property Casualty Insurers Association of America
Securities Industry & Financial Markets Association (SIFMA)
Semiconductor Industry Association (SIA)
Software and Information Industry Association (SIIA)
TechNet
Telecommunications Industry Association (TIA)
TheCityUK
United States Council for International Business
U.S. Chamber of Commerce
US-China Business Council

cc: Minister Gao Hucheng
Ministry of Commerce
2 Dong Chang'an Jie
Beijing 100731
People's Republic of China