

**COMMENTS FROM THE EUROPEAN UNION REGARDING NOTIFICATION
G/TBT/N/CHN/1172
PROVISIONS ON INSURANCE SYSTEM INFORMATIZATION**

The European Union (EU) would like to thank the authorities of China for providing the opportunity to comment on the draft Provisions on Insurance System Informatization notified on 19 April 2016.

The EU would like to raise the following general and specific comments.

1. General remarks

The EU notes that a previous draft of the Provisions was subject to public consultation by the China Insurance Regulatory Commission (CIRC) until 31 October 2015. The EU sent comments to China by the deadline.

The EU appreciates that the CIRC has addressed some EU comments in the notified draft, notably by removing the obligation to use domestic cryptography products and services (Article 54) and by giving some flexibility to insurance companies with appropriate testing capability to carry out in-house performance and security tests (Article 22).

Concerning the other draft provisions, the EU would like to reiterate the comments that remain unaddressed and comment on other aspects which raise concern with regard to the obligations of the TBT Agreement, as outlined below.

The EU acknowledges the need to reinforce network and information security in the insurance sector. Cybersecurity risks are emerging in the financial sector; industry and regulators need to respond to these new threats. Cyber threats are continuously evolving and have become complex. It requires sophisticated advanced technology measures to counteract them.

The management of cybersecurity risk is a global challenge, and an area in which the EU itself takes a close interest. Our fundamental position in the development of EU cyber-related policy is to be geographically neutral; for example, it is not required that EU businesses segment certain activities in the EU, nor do we favour EU products or solutions. The EU would expect similar treatment from our global trade partners.

New policies to help mitigate cybersecurity risks in the financial sector, and in the insurance sector in particular, need to be workable in a global business environment and avoid fragmenting or distorting global markets. They also need to carefully respect the proportionality principle enshrined in particular in the TBT Agreement; policies should not unduly hamper economic growth and innovation; policies need to be in line with international best practices, reflect ongoing discussions at international level (e.g. in the Financial Stability Board), and fully live up to obligations under World Trade Organisation (WTO) rules.

While the provisions of the notified draft are of a fairly general nature, they address, sometimes in a very prescriptive way, various aspects related to the quality management processes of insurance companies. In this area, the EU would encourage China to avoid

regulation of the internal organisation of companies and to focus on a limited number of well justified substantial obligations and deliverables.

2. Specific comments

2.1. Multi-level protection scheme (MLPS) Classification

Article 20 and Article 56 of the notified draft refers to the need to classify information systems in accordance with the MLPS. The EU is concerned that a possible mandating of MLPS level three and above would amount to a ban on procuring foreign ICT products and services for use in such core systems. This in our view would not be in accordance with the proportionality and necessity principles enshrined in the TBT Agreement.

The EU would like to ask the Chinese authorities to clarify which security level within the MLPS is referred to in these provisions.

2.2. Secure and controllable

Article 53 of the notified draft refers to "*secure and controllable hardware equipment and software products*" and appears to mandate the gradual phasing out of all such hardware equipment and software products that are not deemed to be "*secure and controllable*". It furthermore appears to mandate a gradual mainstreaming of capabilities conducive to achieving a "*secure and controllable*" IT environment in an insurance company's informatisation activities.

The EU would like to ask the Chinese to clarify the intended meaning of this Article as it remains unclear what is and what is not regarded as "*secure and controllable*" by the CIRC. The EU underlines that similar concerns have been expressed together with other jurisdictions and stakeholders regarding the currently suspended "*Guidelines for promoting the application of secure and controllable information technology in the banking sector 2014-2015*". Furthermore, the EU would welcome clarification on whether the CIRC intends to elaborate a catalogue of products; the EU would like to underline yet again that the dissemination of the catalogue for IT Guidelines in the banking sector set a bad precedent.

2.3. Source code protection

Article 21 of the notified draft can be read as mandating insurance institutions doing business in China to insist on source code ownership/disclosure from their ICT vendor companies. Mandatory disclosure of source code would amount to mandating the disclosure of business secrets that are essential to the continued successful operation of ICT vendor companies, which has the potential to disrupt trade.

Furthermore, Article 55 seems to require special protection for indigenous intellectual property owned by insurance institutions, which might counter the principle of non-discrimination enshrined in WTO agreements.

The EU would like to ask the Chinese authorities to clarify the intended meaning of these Articles and in particular clarify in which ways intellectual property rights of ICT vendor companies will be protected.

2.4. National/international standards

Article 25 of the notified draft refers to "*national standards*" and makes compliance with them mandatory. The Article does not, however, clearly reference the "*national standards*" in question.

The EU notes that international standard setting bodies are currently working on cybersecurity issues. The EU is concerned in this context that references to Chinese "*national standards*" may not reflect ongoing developments. This reference to "*national standards*" also raises questions regarding compatibility to standards that are internationally in use and accepted. Strict references to "*national standards*" may separate the Chinese market for ICT products and services for insurance institutions from the wider market leading in turn to a fragmented marketplace.

The EU would like to ask the Chinese authorities to clarify the intended meaning of this Article and other references to "*national standards*" in the notified draft. The EU invites the Chinese authorities to use existing global standards (e.g. ISO, Common Criteria). The EU would like to ask the Chinese authorities to confirm that compliance with these "*national standards*" would not require insurers to procure and use only domestic products or technology.

2.5. Areas where further clarification is needed

Articles 22, 41, 54, 81 of the notified draft make reference to third parties, other regulations, laws or accreditation and/or licensing practices. These articles do, however, not clearly reference the respective texts or bodies. Therefore, the EU would like to ask the Chinese authorities to clarify these references.

Likewise, the scope and nature of the "*penetration tests*" mentioned in Article 81 of the notified draft are not defined.

Article 8(h) of the notified draft appears to refer to requirements to store and/or process data only within the territory of the People's Republic of China – a form of geolocation requirement. It is not clear how cross-border data traffic, which is also referred to in Article 58 for "foreign invested" institutions, would be impacted. Global businesses need to be able to transfer data to (and indeed potentially store data in) different locations, for commercial, security and supervisory purposes. Geographical neutrality is needed for information security policy to work in a global environment. The EU would welcome clarification from the Chinese authorities on this provision.

2.6. Date of adoption

In its notification, China indicates that the planned date of adoption coincides with the final date for comments from WTO members, which would prevent those comments being taken into account, thus contravening Article 2.9.4 of the TBT Agreement.

The EU would be grateful if the above-mentioned comments could be taken into account and replied to.