DIGITALEUROPE and European Services Forum (ESF) response to the Draft Supervision Rules on Insurance Institutions Adopting Digitalised Operations

Brussels, October 2015

INTRODUCTION

On behalf of the European Industry, DIGITALEUROPE and ESF welcome the opportunity to provide comments on the *Draft Supervision Rules on Insurance Institutions adopting digitalised operations* (below, the *draft regulation*). Our members – world's leading companies – recognise the strong potential of the Chinese market, as driven by recent Government policies promoting the take-up and the integration of ICT and related technologies in every day life in China.

Over the past thirty years, China achieved tremendous economic success by attracting foreign direct investments in many sectors. We welcome positively initiatives aiming at improving trade, notably the plurilateral and bilateral trade negotiations ongoing (expansion of the Information Technology Agreement, EU-China Bilateral Investment Treaty). We also understand the current challenges for China to counter security threats and fully respect China's interest to ensure privacy and security in the country.

As we noted in our response to the Draft Security Law public consultation which closed August 2015, we believe new information security framework is important for enhancing the security of the country's online ecosystem, in particular as it for the first time codifies cybersecurity rules and requirements at a national level, and indicates a process to define a centralisation of authorities that will be responsible for ensuring successful implementation across the different critical sectors, introducing new levels of clarity and transparency. This approach follows similar developments across the world, where countries have over the past two years began to proactively develop cybersecurity baselines and risk management strategies for their critical and government sectors.

Standards and best practices play a key role in improving cyber security and cyber defence on the international level. Cybersecurity requirements should be voluntary and based on international standards. Mandating technology dependent standards or specific technology does not reduce cybersecurity risks and instead limits flexibility of organisations to respond effectively to rapidly evolving threats. While there should be support for threat information sharing across the public and private sectors, public disclosure of security breaches should be proportionate to the risks involved; disclosures should avoid unnecessary harm to the reputation and confidential information of affected organisations.

Standardisation processes and procedures based on standards and best practices are essential to achieve effective cooperation in cross-border and cross-community environments.

One key point that has emerged from our industry engagement with governments is that the most effective ways of increasing the overall cybersecurity of the online ecosystem are always proportionate, risk-based and prioritised. These approaches focus on protecting what is truly critical to a country's economy, security, public health and citizen's safety.

As more countries introduce cybersecurity related policies, it is important to keep in mind that legislators must carefully balance the impact of the policies on a country's national security and public safety with its potential impact on global trade, technology innovation and the benefits of informatisation.

While the government always needs to focus on national security and protecting the public interest of the people in its decisions, overly restrictive laws or regulations can hinder the ability of multinational companies to bring advanced technologies to countries like China and to further invest in China. The result will be a diminished access to novel technology approaches and decline in cybersecurity protections.

It would result in a less competitive Chinese market with fewer choices available to the Chinese customers and users. A likely result would also be a further challenge to a country's continued modernisation, as it could result in reciprocal legislation

abroad and therefore limit the ability of the Chinese companies to compete on equal terms internationally.

We would encourage legislators to further clarify some key concepts and definitions in the draft regulation, adopt international standards and best practices, and reconcile the draft regulation with other existing laws and regulations. We also recommend that in further developing the draft regulation and the implementing regulations, the legislators engage and partner with IT providers and Insurance companies to determine technical viability of the requests into consideration so as to avoid putting unnecessary and unviable burdens on businesses, whilst retaining the ability to reach their objectives.

DIGITALEUROPE and ESF would like to present several recommendations to ensure that the scope and provisions of the draft regulation will achieve its primary objectives without hampering the capacity of the digital industry in China to invest, innovate, research, develop and produce in the country. We would also like to encourage the Government of the People's Republic of China to acknowledge and recognise the principles of the Global ICT Industry Statement with recommended Government approaches to cybersecurity (June 2012, http://www.itic.org/dotAsset/51ad6069-9f1b-4505-b2ff-b03140484586.pdf).

1. Clarifications needed

DIGITALEUROPE and ESF are of the opinion that the draft regulation should further clarified the definition and scope of several provisions, notably:

- Article 19 (Regulatory framework) states that an insurance institution shall notably « develop the management rules, technical standards and operational norms covering the entire life cycle of information systems ». We believe this provision might create a confusion in the distribution of responsabilities between Insurance institutions and CIRC.
- Article 20 (Classification of Security levels) assigns the use of « higher security levels » for core systems containing information involving national security, the institution's business secrets and user privacy. The draft regulation should clarify what these higher security levels should imply.
- Article 21 (forms of development) promotes indigenous R&D capabilities and allows for joint R&D and outsourcing only if the Insurance

Institution has the rights to possess of authorized use or own the source codes. Such IP is business proprietary information that is essential to companies ability to innovate and remain economically competitive.

- Article 22 (Development and testing) requires the testing of functions, performance and security of information systems before its operation. It also allowed third party institutions to conduct the tests. We would welcome examples for the classification of information systems mentioned in the provision. A list of certified third party should be provided/annexed to the draft regulation. This could include intrusive inspections of systems or products used in critical infrastructure, compromising key intellectual property. These should be performed in a manner that is as minimally intrusive to user interests as reasonably possible, respectful of proprietary information, trade secrets and intellectual property, and subject to auditing and oversight to minimise the potential for abuse. Assessment of security vulnerabilities should be based on the technically features of the networks and equipment being evaluated, and not based on the product brand or country of origin. CIRC should allow for compliance requirements based on risk assessments, and be supportive of international transportability of test results and certificates.
- Article 23 (1) calls for an «appropriate ID authentification mechanism ». It should be clarified what this exactly means.
- Chapter 4 (Infrastructure, Construction and Assurance): this chapter also requires companies to have a data center located within China when data comes from within the territory of China (Article 31). Given the importance of global nature of the Internet based economy, restricting data flows and requiring local storage will be problematic for both international and domestic service providers and their customers. Such restrictions would limit access by Chinese companies to leading technology services and would impede their ability to operate in global markets, thus reducing their competitiveness and ability to grow. Location of data storage does not ensure cybersecurity; access to the most advanced security technologies and how those technologies are implemented, both for data at rest and in transit is more important. The law may consider adopting language to support security innovation to enhance data protection (outcome driven), rather than to restrict the location of data storage and usage.

- Article 53 (Security and controllability) – in connection with article 25(2) - states that « an insurance institution should give priority to purchasing secure and controllable hardware equipment and software products, to advance application of secure and controllable products stably ». As for the previous draft on new banking regulations, we strongly recommend CIRC to clarify the notion of « secure and controllable ».
- Article 54 (Domestic cryptography) requiring domestic cryptography could serve as a trade barrier. It would be preferable to allow for equivalent alternative offerings from other countries within parameters and classification categories provided in international standards.
- Article 55 (Software legalization) enhance « indigenous IP protection awareness ». We would strongly suggest to provide clarification on the objectives of this provision.
- Article 56 (Multi-level protection) : We would welcome some clarification on what the process is.
- Article 57 (Security certification) : This provision requires Insurance Institutions to sign a safety and confidentiality agreement with certification bodies accredited for certifications of compliance. It is important for operators to understand what kind of clauses this agreement would include.
- Article 58 (Data security) :further clarification should be provided on the « appropriate laws and regulations » data carried by information systems beyond the border of China shall be complied with. As one of the most important security programs governing cybersecurity, MLPS needs to evolve and be integrated/aligned with other security programs to resolve overlaps and ambiguity across different programs.
- Article 82 (Joint supervision): Supervision and management of the information systems of Insurance Institutions are expected to be developed by the CIRC according to chapter 9. However, article 82 states that the CIRC and the National Information Security Department may build a joint supervision mechanism to exercise effective supervision for the matters concerning information security supervision over outsourcing service providers. We would like to obtain a clear definition of the kind of matters mentioned in the provision which could be subject to joint supervision. We also insist that a level of coordination will be critical to ensure unnecessary

duplication of information, as well as request and requirements on the private sector.

2. Recommendations on Industry's involvement and adopting international standards and best practices

2.1. International standards and best practices

An open and collaborative cyberspace is critical to ensuring its security. We would particularly like to see a greater emphasis on Chinese participation in development and usage of international security standards and best practices throughout the document and in particular in Article 5 (standard to be followed), Article 25 (security mechanism), Article 31 (Construction standards), and Article 75 (Contents of supervision) which refers to the use of technologies, products and data centers complying with national standards and encryption requirements.

This will allow for a greater information exchange and ensure that China is able to access the latest in security technology developments. Shifting the focus of the draft regulation slightly to a desired end-state approach rather than prescribing the means to achieve it, as a greater utilisation of international standards would enable, would also enable innovation in the marketplace and discourage organizations from adopting a "tick-box" approach to compliance. It would also ensure that the draft regulation can stand the test of time and remain current in the future despite the fast pace of innovation in the marketplace. When it comes to development of domestic standards, as proposed in Article 5 we recommend that the government allows for and encourages foreign participation in the process to ensure the final product does not inadvertently result in a market barrier.

Moreover, we would advise the government to streamline the cybersecurity standard system they are developing to ensure a clear set of requirements emerges rather than a patchwork of competing proposals. The law should therefore focus on international and national standards, and avoid the proliferation of specialised industry standards and regulations, which would lead to diffusion and ambiguity in requirements, and as a result, to diminish security and inhibit the healthy development of informatisation in the economy and society. Enterprises establishing enterprise standards will further compound such negative results.

2.2. Industry's involvement

We believe private sector's participation will be key to the success of the implementation of this draft regulation. Unfortunately, the current draft does not account for private sector participation despite the integral role the private sector plays in maintaining and operating many of the systems. In particular, the private sector should be involved in the circulation of early warnings on risks and incidents. For example, the government should ensure that the affected industry player is consulted before issuing a warning on risk and incidents. This is critically important when it comes to sharing information about security vulnerabilities. In line with industry practice and to minimize security risk, these should not be widely disclosed before they are fixed.

CONCLUSION

We firmly believe that a positive dialogue between China and the EU is a key condition to ensure and promote investment in technology development, innovation and deployment, which together would greatly benefit the ICT industry worldwide, including Europe and China and the digital economy as a whole. Boosting EU-China trade guided by reciprocity and a fair and open market access is a win-win situation for China and Europe.

We are very much looking forward to working with you on a positive and comprehensive digital policy that will promote investment, innovation, research, development and production in China.

DIGITALEUROPE

ESF
European Services Forum

--
For more information please contact:

- Pascal Kerneis, Managing Director at European Services Forum
  +322 230 75 14 or p.kerneis@esf.be

- Diane Mievis, Senior Policy Manager Global Economic Affairs at DIGITALEUROPE
  +32 2 609 53 23 or diane.mievi@digitaleurope.org

ABOUT EUROPEAN SERVICES FORUM

The **European Services Forum (ESF)** is a private sector trade association that represent the interests of the European services industry in International Trade Negotiations in Services & Investments.

It comprises major European service companies and European service sector federations covering service sectors such as banking and insurance services, tourism, telecommunications, maritime transport, IT, business and professional services, distribution, postal and express delivery, IT service (see full list of members on the web-site: www.esf.be)

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 59 corporate members and 36 national trade associations from across Europe. Our website provides further information on our members, recent news and activities: http://www.digitaleurope.org