European Chamber
中国欧盟商会

Comments on the CIRC <Supervision Rules on Insurance Institutions Adopting Digitalized Operations>
中国欧盟商会对保监会《保险机构信息化监管规定（征求意见稿）》的建议

Introduction
介绍

The European Union Chamber of Commerce in China (European Chamber) is pleased to comment on the *Supervision Rules on Insurance Institutions Adopting Digitalized Operations (Draft for Comments) ('(draft) Supervision Rules')* and appreciates that this call for comments was launched publicly by the China Insurance Regulatory Commission (CIRC).

中国欧盟商会（欧盟商会）很高兴能够对《保险机构信息化监管规定（征求意见稿）》（《监管规定》草案）提出意见，并感谢中国保险监督管理委员会（保监会）公开发布了此征求意见稿。

The European Chamber supports China's desire to create a secure and reliable operating environment for insurance institutions. To this end, we first emphasize some general comments for addressing cybersecurity related legislation in the insurance sector:

欧盟商会支持中国为保险机构创建一个安全可靠运营环境的迫切期望。为此，我们希望首先强调几点针对保险业网络安全立法的总体建议：

1. Market-based solutions
市场化解决方案

Using a market-based approach, i.e. allowing insurance companies to freely choose the cyber security products and solutions to fulfill their security needs is recognized as the most efficient way to ensure a consistently high security level for the system overall. This is because market-based competition between insurance companies necessitates them to continuously invest in their security, simply for fear of losing out to a competitor. The CIRC, as a regulator, should harness this natural process more effectively, through refraining from prescriptively laying out procurement requirements. Mandating the use of localised or indigenously developed platforms, products or solutions is detrimental to overall system security, as it risks increasing the number of attack surfaces and constrains the interoperability

of a company's systems, inside and outside of China. Furthermore, leveraging standards that are based on global best practices and experiences will allow industry to incorporate regular updates to their systems and develop their security needs apace with the evolution of cyber security threats.

采用市场手段，即允许保险公司通过自由选择网络安全产品和解决方案满足其安全需求，被认为是确保系统整体保持高安全级别最为有效的方法。这是因为保险公司间的市场竞争要求他们在安全领域进行持续投入，以防被竞争对手淘汰。作为监管部门，保监会不应强制规定采购要求，如此才能实现对这一自然过程更为有效的监管。不论在中国还是中国之外，强制使用本地化或自主开发的平台、产品或解决方案都将增加攻击次数、限制同一公司不同系统间的互操作性，从而有损系统整体安全。此外，采纳与全球最佳实践和经验一致的标准可使行业将定期更新纳入其系统，并使其安全需求与变化中的网络安全威胁相适应。

2. Transparency and Public Consultation
透明度及公开征求意见

Ensuring that the policy-making process is conducted in a transparent manner with public consultation, such as this call for comments, will help the CIRC and the business community. By doing so, businesses will better understand issues of concern of regulators, contribute to solutions, and eventually ensure compliance as well. We thus recommend to the CIRC to continue to publicly release its revised (draft) Supervision Rules at the drafting stage for comment and to give sufficient time for formal feedback, ideally 30 days, prior to any implementation. This should apply to any other forthcoming documents related to the (draft) Supervision Rules, such as add-on notices or catalogues clarifying which information technology (IT) products and solutions are under the jurisdiction of the (draft) Supervision Rules. We noted with concern that an unfortunate precedent was set earlier this year with the roll-out of a set of guidelines to regulate the procurement of IT products and solutions in the Chinese banking sector. In that case, a product catalogue with vital information on the product categories affected was never officially made public. In this respect, we would like to reiterate the need for transparency in legislation and involvement of all stakeholders, domestic and international.

确保政策以透明方式制定，并以诸如本征求意见稿等方式进行公开意见征集，将同时使保监会及业界获益。这样，企业方可更好地理解监管机构所关心的问题，更有针对性地提出解决方案，并最终保证合规。因此，我们建议保监会继续在制定阶段公开发布《监管规定》修订征求意见稿，且在实施前为正式反馈预留足够时间，以 30 日为佳。这一规定应适用于未来任何有关此

《监管规定》草案的文件（如附加通知或目录，明确何种信息技术产品及解决方案适用于《监管规定》）。我们注意到，今年年初出台的针对中国银行业采购信息技术产品及技术方案的管理规定创下了一个负面先例：含有产品分类重要信息的受影响产品的目录从未被正式公开。为此，我们希望重申立法透明度和保障所有国内外利益相关方参与度的必要性。

Specific Comments
具体建议

The *(draft) Supervision Rules* include several articles and provisions that are a concern for European industry, due to several requirements stipulated therein:

《监管规定》草案包括了欧盟企业关心的数条条款，归因于条款中所含的以下要求：

- Requirements to use **indigenously developed cryptographic solutions**
  要求使用**自主开发的加密方案**

Article 54 of the *(draft) Supervision Rules* appears to require China-based insurance companies to progressively shift their procurement of cryptographic products fully towards indigenously developed solutions, thereby phasing out foreign suppliers. Aiming for exclusive reliance on domestically developed products and solutions and prescriptively laying out technologies deemed to be fit for procurement—as the *(draft) Supervision Rules* intend to do—increases the technology risks posed to the system overall, as well as it eventually leads to technology insularity. We believe that enforcing such a measure could serve to effectively bifurcate the market for cryptographic products into a Chinese and a global one.

《监管规定》草案第 54 条要求中国境内保险公司逐渐将其采购的加密产品转移到自主开发的解决方案，由此逐步淘汰外国供应商。《监管规定》草案中涉及的仅依赖本国开发的产品和解决方案、规定可被纳入政府采购框架的技术的做法，将提高整体系统的技术风险，并最终导致技术孤立。我们相信实施此类措施将事实上导致中国加密产品市场和国际市场的分化和隔离。

- The apparent requirement for **data localisation**
  对**数据本地化**的明确要求

Article 8 (8) appears to mandate that company data is stored and processed only within the territory of the People's Republic of China. The vague formulations of the article insinuate that this is indeed a concern. It furthermore does not clarify how cross-border data flows would be dealt with. In this the worst case, this article could have a strong negative impact on insurance companies global business operations.

第 8 条第 8 款似乎强制规定了企业数据仅限在中华人民共和国境内进行保存和处理，但其模糊的措辞显示，这一担忧并非空穴来风。此外，该条款并未明确指出应如何处理跨境数据流通。在最坏的情况下，其或会对保险公司全球商业运营产生严重负面影响。

- The **Multi-Level Protection Scheme**
  等级保护体系

Articles 20 and 56 make reference to China's already established multi-level protection scheme (MLPS), which tiers sectors into an ascending order with five levels according to their significance for national security, with Level 3 and above being deemed critical to national security. We are concerned that mandating the MLPS for IT systems in the insurance sector could amount to a gradual phasing out of foreign suppliers. We observe that insurance is a purely commercial sector and respectfully ask the CIRC to clarify, which MLPS level IT system in the sector would fall under.

第 20 及第 56 条提及中国已经建立了等级保护体系，该体系根据对国家安全的重要性按升序方式将不同行业分为五个级别，第三级及以上的行业被视为与国家安全密切相关。我们担忧，在保险业内对信息技术系统启用等级保护体系会逐步排挤掉外国供应商。我们观察到，保险业是一个纯粹的商业部门。因此，我们谨希望保监会可就信息技术系统在该等级保护体系中的级别进行澄清。

- **"Secure and controllable"**
  "安全可控"

Article 53 invokes the requirement for products and solutions to be "secure and controllable", and appears to mandate a gradual shift of procurement away from products that do not comply with any criteria against which their 'security and controllability' is measured. As far as we understand, no supplementary documentation outlining the criteria by which a product is deemed to be "secure and controllable" has been published. We sincerely hope that the CIRC will clarify what it means by "secure and controllable" and that it will impartially inform all stakeholders of this.

第 53 条提出产品及解决方案应"安全可控"的要求，且似乎要求逐渐停止对所有不符合"安全可控"要求的产品的采购。据我们所知，目前尚未有任何公开发布的附加文件显示判断"安全可控"的依据为何。我们谨希望保监会可澄清"安全可控"的含义，并将其公平地告知所有利益相关方。

- **Source code disclosure**
  源代码披露

We are concerned by the vague formulations in Article 21, which appear mandating China-based insurance companies to require their IT providers to disclose the source code of their products. The requirement to disclose source code is a strong concern for European industry. We urge the CIRC to delete any requirement for source code filing from the *(draft) Supervision Rules*.

我们对第 21 条含糊的措辞表示关注。该条似乎强制中国境内保险公司要求其 IT 供应商披露源代码信息，欧洲企业对此十分关切。我们强烈要求保监会从《监管规定》草案中删除任何有关对源代码备案归档的要求。

- **National and international standards**
  国家及国际标准

Article 25 (2) makes references to domestic Chinese national standards and appears to make compliance with them mandatory. However, it is not clarified which national standards are exactly being referred to. We note that mandating national standards could serve to disconnect the Chinese from the global market, and thus weaken the security of the Chinese insurance system. Globally consistent solutions are required to ensure interoperability between the systems of insurance companies, whether across any company's international branch network or from one company to another. Moreover, cybersecurity risks go beyond national borders, highlighting

the need for cooperation between a multitude of stakeholders such as national and supranational government agencies, national and multilateral supervisory institutions, industry associations, standardisation organisation and the private sector alike, to work together to develop benchmark solutions that ensure the integrity of integrated global markets and their constituent actors is adequately protected against cyber threats. To this end, an open discourse between all these different stakeholders is simply a necessity.

第 25 条第 2 款提到要强制符合中国国家标准，然而并未列明哪些国家标准应被遵守。我们认为强制推行国家标准可能会中断中国与国际市场的联系，由此降低中国保险业的系统安全。若想确保保险公司系统间的互操作性（包括不同公司间及同一公司不同分支机构间），则应采用国际统一的解决方案。此外，网络安全风险超越国界，因此需要国家及超国家政府机构、国家及多边监管机构、行业协会、标准化组织和私企等不同利益相关方间展开合作，共同开发能够保障统一全球市场完整性、使市场构成主体不受网络威胁侵袭的基准方案。为此，这些利益相关方间的公开对话尤为必要。

- **Vaguely defined concepts and references to be clarified**
  泛泛的定义及涉及内容亟待明确

Several articles, including Articles 22, 41, 54, 81, etc. make vague references to “third parties”, “other regulations”, “licensing practices” and so on. However, at no point in the document are these terms further clarified. We are concerned by the general lack of clarity inherent to many of the articles and respectfully urge the CIRC to provide clear definitions of any of these terms.

包括第 22、41、54、81 条在内的某些条款泛泛地提及了“第三方”、“其他法规”、“批准”等。然而，征求意见稿并未对这些术语进行进一步解释。我们对许多条款中普遍存在的缺乏明确性的问题表示担忧，并谨希望保监会能够就这些术语提供更明确的定义。

For these reasons, we encourage the CIRC and other relevant departments of the Chinese Government to revise the *(draft) Supervision Rules* in such a manner that they do not preclude China-based insurance companies or those considering setting up operations in the country, from procuring products and solutions from vendors across the global marketplace. We believe that restricting the procurement

choices of insurance companies to indigenously developed products and solutions and to deliberately favour the domestic providers of these, will ultimately risk compromising the overall security of information systems in the Chinese insurance sector.

基于上述原因，我们鼓励保监会及其他中国政府相关部门对《监管规定》草案进行更为彻底的修订，以确保新规不会阻碍中国境内或希望进入中国市场的保险公司在全球市场上向供应商采购产品及解决方案。我们相信，将保险公司的采购选择局限于自主开发的产品及解决方案并蓄意偏袒国内供应商，最终可能危害中国保险业整体的信息系统安全。

We, representing European industry in China, note that EU-China relations have grown from strength to strength this year with numerous successfully held bilateral high-level meetings and visits such as the EU-China Political Summit, EU-China Business Summit, the High Level Economic Dialogue amongst many others at the member state level.

欧盟商会及其所代表的欧洲在华企业注意到，今年中欧关系随着多次成功的双边高层来访、会晤而不断向良性发展，如中欧政治峰会、中欧工商峰会、高层经济对话，以及其他一些同成员国层面上的活动。

We are encouraged by the commitments that both the EU and China have made to transparency and non-discrimination. These commitments can be best honoured by ensuring that drafting of the *(draft) Supervision Rules* is conducted in precisely such a manner.

我们很高兴看到中欧双方承诺坚持非歧视及透明原则，而履行承诺的最佳方式便是确保《监管规定》草案制定过程能够遵循此种精神。

Conclusion
结语

We highlight that mandating China-based insurance companies to procure the products and solutions in accordance with the *(draft) Supervision Rules* would ultimately be to the detriment of the overall cybersecurity of the Chinese insurance system. We believe that it is important for the CIRC to recognise the risks arising from these issues at the outset and to thoroughly revise the *(draft) Supervision Rules* in turn.

我们希望强调，强制要求中国境内保险公司采购与《监管规定》草案相符的技术产品及解决方案最终会降低中国保险业整体网络安全性。我们认为，保监会有必要从一开始便认识到这些问题所带来的风险，并致力于对《监管规定》草案进行彻底修订。

As different information technology standards develop, the evolution of cyber threats continues apace. The most effective approach to developing policies to govern the insurance sector and to ensure that its information technology systems are secure, is to base the drafting of any regulations on open and transparent formulation and implementation, encompassing the public dissemination of these draft regulations including all supplementary documentation, such as product catalogues, to allow both domestic and international stakeholders to provide input and advice to the regulator.

随着各类信息技术标准的发展，网络安全威胁也处在不断发展变化当中。制定保险业监管政策、保障行业信息技术系统安全性最行之有效的方法是确保有关法规的制定过程中，起草和实施环节都能够公开透明。这包括公开法规草案（含产品目录等附加文件），并允许国内外利益相关方向监管机构提出意见和建议。

Insurance companies have a natural incentive as dictated by the market, to invest in the best technology solutions and to ensure that their systems are secure. As such, it is vital that they are allowed to conduct their own risk assessments as well as to autonomously determine how best to ensure that their systems are secure. Enabling such self-assessment has to be the end-goal of any effective prudential framework to govern technology and cyber security risks in the Chinese insurance sector.

出于市场竞争本能，各保险公司自然都会选择最佳技术方案以确保其系统安全运行。因此，当下最重要的是允许各保险公司进行自我风险评估并自行决定如何最佳维护系统安全。不论中国保险业建立何种谨慎有效的网络安全风险及技术管理体系，其最终目标都应该是启用此类自我评估机制。

We hope that the CIRC proactively engages in consultation with its peer supervisory organisations in other jurisdictions and to share—and when appropriate to adopt—international best practices.

我们希望保监会能够积极与其他国家同行监督机构进行磋商，学习国际最佳实践，并适时采纳有关实践。

We once again thank the CIRC for the opportunity to comment and stand ready to support the CIRC in the further revisions of this draft.

谨此，我们再次为能有机会对草案进行评论向保监会表示感谢，并也做好准备随时为保监会对该草案进一步修订提供支持。

—END—

—完—