Cyberspace Administration of China,

国家互联网信息办公室

No. 11, Che Gong Zhuang Da Jie, Xicheng Qu

北京市西城区车公庄大街 11 号

Beijing Shi, People's Republic of China

北京市，中国

security@cac.gov.cn

24 June 2019

2019 年 6 月 24 日

Dear Sir/Madam

尊敬的先生/女士:

RE: The Consultation Draft of the Measures on Cybersecurity Review

关于：《网络安全审查办法》征求意见稿

The Global Financial Markets Association ("**GFMA**")[1] welcomes the opportunity to submit comments and suggestions on the Measures on Cybersecurity Review *(《网络安全审查办法》)* (the "**Review Measures**"), issued by the Cyberspace Administration of China (the "**CAC**").

全球金融市场协会（"**GFMA**"）很荣幸有机会就国家互联网信息办公室（"**贵办公室**"）发布的《网络安全审查办法》("**《审查办法》**")提出意见和建议。

GFMA members appreciate the efforts made by the CAC to update the Measures on Network Products and Services Security Review *(《网络产品和服务安全审查办法（试行）》)* issued in 2017 (the "**Existing Measures**") and provide more specific guidance on

[1] GFMA brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London and Brussels, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, please visit http://www.gfma.org

GFMA 汇集了三个世界领先的金融贸易协会，以应对日益重要的全球监管议程，并促进协调一致的倡导工作。位于伦敦和布鲁塞尔的欧洲金融市场协会（AFME），位于香港的亚洲证券业和金融市场协会（ASIFMA）以及位于纽约和华盛顿的证券业和金融市场协会（SIFMA）分别是 GFMA 的欧洲，亚洲和北美成员。 有关更多信息，请访问 http://www.gfma.org。

the content of cybersecurity review as well as procedures of such review. We believe this consultation draft has addressed some of the concerns raised by the industry in relation to the Existing Measures and will contribute towards building a robust market.

GFMA 会员感谢贵办公室对 2017 年颁布的《网络产品和服务安全审查办法》("**现行办法**")所做的更新，以及对网络安全审查的内容和程序提供更详细的指导。我们相信，这份征求意见稿回应了业内人士对现行办法提出的关切，并将促进建立稳健的市场。

In this letter, we seek clarification on the application of, and respectfully suggest amendments to, certain provisions of these Review Measures.

在本函中，我们希望明确《审查办法》中部分条款的使用情况，并谨对部分条款提出我们的修订建议。

1. Scope of Critical Information Infrastructure

1. 关键信息基础设施的范围

The Review Measures focus on securing the critical information infrastructure ("**CII**") by requiring CII operators ("**CIIO**") to conduct security review on products and services. The concept of CII was firstly proposed two years ago, however, its scope remains unclear. We would appreciate clarity on the scope of CII and the specific guidelines on how to identify any CIIO. We also suggest the Review Measures be formally issued after the scope and identification of the guidelines of CII are clarified; otherwise, it would be difficult to fully assess the impact of the Review Measures.

《审查办法》着重讨论通过要求关键信息基础设施运营者对产品和服务进行安全审查的方式，确保关键信息基础设施的安全。关键信息基础设施的概念最早于两年前提出，但至今该定义的涵盖范围仍不清楚。我们希望能够澄清关键信息基础设施的范围以及提供有关如何认定关键信息基础设施运营者的具体指引。我们还建议，在关键信息基础设施的范围及其识别指引正式发布之后，再正式发布《审查办法》，否则将难以全面评估《审查办法》的影响。

2. Impact on Non-CIIOs

2. 对非关键信息基础设施运营者的影响

Article 19 of the Review Measures states that where any purchase of network products and services or any information technology service is believed by the member of the cybersecurity review working mechanism (including various governmental agencies such as the central bank, and national security authority) to affect or potentially affect state security, the Cybersecurity Review Office will organize a cybersecurity reviewing in respect of such purchase or service after obtaining approval from the Central Cyberspace Affairs Commission in accordance with certain procedures.

《审查办法》第十九条规定，网络安全审查工作机制成员单位（含中央银行和国家安全机关等各类政府机关）认为网络产品和服务的采购活动或信息技术服务影响或可能影响国家安全的，网络安全审查办公室将在按程序报中央网络安全和信息化委员会批准后，安排对该等采购或服务组织网络安全审查。

This article seems to indicate that non-CIIOs may also be subject to the cybersecurity review under certain circumstances, however, the description on the criteria and procedure to determine if a non-CIIO should be caught under this article is unclear. We believe that, as a general principle, non-CIIOs should be exempted from cybersecurity review. Therefore, we respectfully suggest the removal of this article or, if this article is critical, specifying only limited and exceptional circumstances that non-CIIO may be subject to the cybersecurity review, and to what extent the review will apply in each case. We also suggest that the definition of what affects or may affect state security be clarified as it may

be subject to different interpretations. At least some criteria to make the determination should be provided.

该条款似乎表明，在某些情况下，非关键信息基础设施运营者也可能需要进行网络安全审查，但关于非关键信息基础设施运营者是否受限于本条的判定标准及判定程序的表述尚不清晰。我们认为，作为一项一般性原则，非关键信息基础设施运营者应被豁免进行网络安全审查。因此，我们谨建议删除此条款，或者在此条至关重要的情况下，明确只有在有限或特殊情形下非关键信息基础设施运营者才可能需要进行网络安全审查，以及明确在各类情形下安全审查的程度。我们还建议，对于"影响或可能影响国家安全"的定义应予以澄清，因为它可能会导致不同的解读，或应至少提供一些判断的标准。

3. Concept of "massive personal information and important data"

3. "大量个人信息和重要数据"的概念

Article 6 of the Review Measures requires a cybersecurity reviewing be conducted by the Cybersecurity Review Office if there is a possibility of divulging, loss, damage or cross-border transfer of "massive personal information and important data." It would be helpful if the scale of data that constitute "massive" and "important data" is defined under these Review Measures. Without these practical guidelines, it would be difficult for companies to comply with Article 6. Therefore, we seek clarification on the following aspects: (1) the quantitative measurement of the term "massive" and (2) the specific scope of "important data" and whether this term bears the same meaning as it is defined in other regulations including, for example, the consultation draft of Measures on Data Security and the consultation draft of Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment; and (3), if a different meaning is adopted, the reason for such differentiation.

《审查办法》第 6 条要求，在"大量个人信息和重要数据"可能出现泄露、丢失、毁损或出境的情况下，网络安全审查办公室将进行网络安全审查。若定义《审查办法》下，何种规模的数据构成"大量"和"重要数据"的含义，将会很有帮助。若没有这些实操层面的指引，公司将很难遵守第 6 条的规定。因此，我们希望从以下几个方面明确:(1)"大量"一词的判断标准，及(2)"重要数据"的具体范围以及该术语是否具有与其他法规中相同的含义，例如《数据安全管理办法》征求意见稿和《信息安全技术——数据出境安全评估指南》征求意见稿;及(3)如果采用了不同的定义，则说明该等区别的原因。

Also we suggest clarifying the potential liability for breach of Article 6. In particular, whether vendors may be deemed directly liable for the failure of network operators in the accurate measurement/review of the potential impact of the relevant products/services.

此外，我们建议明确违反第 6 条规定的潜在责任。特别是，产品/服务提供者是否可能对网络运营者未能准确判断/审查相关产品/服务的潜在影响承担直接责任。

4. Risk factors to be Considered

4. 应考虑的风险因素

Article 10 of the Review Measures sets out the risk factors to consider when conducting cybersecurity reviews, including the possibility of the CII getting manipulated or interfered or its business continuity destroyed, the possibility of the purchase leading to the divulging, loss, damage or cross-border transfer of massive personal information and important data, and whether the product and service provider is funded or controlled by foreign governments.

《审查办法》第十条规定了进行网络安全审查时应当考虑的风险因素，包括关键信息基础设施被控制、被干扰和业务连续性被损害的可能性，购买（网络产品和

服务）导致个人信息和重要数据泄露、丢失、损毁或跨境转移的可能性，以及产品和服务提供者是否受外国政府资助、控制的可能性等。

These risk factors are highly speculative and many products could "possibly" be compromised to result in a breach. It is difficult to assess possibilities for compromise this ahead of time – if a company was certain that there was a possibility for compromise, the company wouldn't buy the networked product in the first place. In addition, the due diligence on-boarding requirement under paragraphs 5 and 6 of Article 10, including reviewing the track record of vendor compliance and identifying the funding and controller of the vendor, will cause delay in procurement. Given the importance of the CIIOs, which are already incentivized to use reliable vendors, we believe these additional requirements are burdensome with no real benefit. Therefore, we suggest removal of paragraphs 5 and 6 and more detailed guidelines to be provided in determining the risk factors to be considered for cybersecurity review.

这些风险因素具有很强的推断性，许多产品"可能"会为达成折中的解决方案而选择违约。目前很难提前评估出现折中的可能性——如果一家公司确信存在折中的可能性，那么公司在最初就不会购买这种网络产品。此外，根据第 10 条第 5 及第 6 款规定的尽职调查要求，其中包括审查产品/服务提供者合规记录以及确定提供者的资金来源和控制人，这将导致采购的延误。考虑到关键信息基础设施运营者的重要性（其将促使使用可靠的提供者），我们认为这些额外的要求过于繁重而并无实益。因此，我们建议删除第 5 段和第 6 段，并在确定网络安全审查需要考虑的风险因素时提供更详细的指引。

5. Approach of Security Review

5. 安全审查的方法

According to the Review Measures, network operators are the obligors to conduct security review on the products and services, and we respectfully suggest reconsidering the approach of such review.

根据《审查办法》，网络运营者是产品和服务安全审查的义务主体。我们建议贵办公室重新考虑安全审查的方法。

First, the current approach is redundant as it would require each network operator to assess risk and secure approval for the same product/service, and for regulators to approve the same product multiple times. Second, this will lead to inconsistent risk review and approval results for the same product/service, as multiple network operators and working-level government officials will be involved in separate approval processes. In addition, the Review Measures do not require authorities to disclose the results or contents of approvals to maintain transparency, which may also lead to inconsistent results.

首先，根据目前的审查方法，每个网络运营商都应评估风险，并确保对相同产品/服务的批准，并且监管机构要多次批准同一产品，这一方法比较冗余。其次，这将对相同的产品/服务导致不一致的风险审核及审批结果，因为不同的网络运营商和不同层级的政府官员将分别参与各个审批流程。此外，《审查办法》未对为保持透明度而公开评审结果或者评审内容作出要求，这同样可能导致各评审结果的不一致。

Overall, the Review Measures would put an undue burden on operators to submit a security review and request review and approval for network products and services. We respectfully suggest requiring vendors, instead of network operators, be responsible for the approval process. Vendors are in the best position to do so as they are specialized in and familiar with their own products/services' capabilities and specifications. Once a product/service is approved, any company should be allowed to use it without having to secure separate approval. If the CAC considers this approach inadequate, we would suggest at least the products/services already passing the security review be published so that a more efficient and transparent review mechanism may be achieved.

总体而言，《审查办法》将因运营者需要提交安全审查并申请对网络产品和服务进行安全审查和批准，而增加运营者不合理的负担。我们谨建议要求提供者而非网络运营商，对审批过程负责。提供者最适合对此负责因为他们对自己的产品/服务的性能及特点非常熟悉。一旦一项产品/服务被批准，任何公司都应该被允许使用它，而不必单独获得批准。如果贵办公室认为这种审查方法不够充分，我们建议至少公布已通过安全审查的产品/服务，以便实现更有效和更透明的审查机制。

GFMA greatly appreciates the CAC's consideration of the points and questions raised in this letter and would be pleased to discuss them in greater detail. If you have any questions, please contact Erik Bainbridge, Manager Policy and Regulatory Affairs at ebainbridge@asifma.org or Tel: +852 2531 6562. This submission was prepared by PRC law firm Fangda Partners, GFMA, and its affiliates' members.

GFMA 非常感谢贵办公室考虑本函提出的观点和问题，并将很乐意更详细地讨论这些问题。如果您有任何疑问，请联系政策和法规事务经理埃里克·班布里奇先生（电邮 ebainbridge@asifma.org 或电话+85225316562）。本函由上海市方达律师事务所、GFMA 以及其会员共同撰写。

Yours sincerely,

顺颂商祺，

Kenneth E. Bentsen, Jr.

CEO, Global Financial Markets Association and

President and CEO, Securities Industry and Financial Markets Association

全球金融市场协会首席执行官 及

证券业和金融市场协会首席执行官兼主席