31 May 2022

致：
中国证券监督管理委员会（中国证监会）
通过电子邮件提交至 kejiju@csrc.gov.cn 和并传真至010 880614444

亚洲证券业与金融市场协会（ASIFMA）对《证券期货业网络安全管理办法》（征求意见稿）的反馈意见

尊敬的先生/女士：

亚洲证券业与金融市场协会（ASIFMA）[1]很高兴有机会就中国证券监督管理委员会（“证监会”）《证券期货业网络安全管理办法（征求意见稿）》（《办法》）提出反馈意见。我们的反馈意见包括两个部分：1）总体意见；2）逐条的具体意见。

总体意见：

与现行规则和条例保持一致

我们建议《办法》与现行的监管要求保持一致，以避免受监管实体产生混淆。我们在下文的逐条反馈意见部分指出，《办法》草案中的许多要求，例如压力测试、性能容量要求和某些数据类型的数据备份要求，在证监会2019年生效的《证券基金经营管理机构信息技术管理办法》（2021年修订）中已经涵盖，《办法》的要求与现行监管要求不一致。

共享敏感数据的风险

《办法》草案重点关注数据安全；但是，在第二十九条、第五十条和第五十二条中，却要求企业为各种目的而共享数据。加强数据安全对所有各方都很重要，尤其是对于那些被授予访问或保管敏感数据和信息的主体。一些数据对于经营机构而言高度敏感，特别是与网络安全有关的信息。这些数据对黑客和其他不法分子极为有用，并可能便于他们直接或通过供应链攻击经营机构和/或行业。因此，我们希望与证监会合作，尽量减少数据收集，减少电子足迹，如果出于监管目的必须收集敏感数据，则寻求其他途径。2021年9月14日，我们曾，就此主题致函国际证监会组织（IOSCO）亚太地区委员会副主席的申兵先生，申兵先生同时也是证监会国际部主任（见附件A）。

渗透测试要求

[1]ASIFMA 是一个独立的地区性行业协会，会员基础广泛，由买方和卖方市场 160 多个领先金融机构组成，包括银行、资产管理人、律师事务所、市场基础设施服务提供商等。我们与各会员共同发掘金融行业的共同利益，推动亚洲各资本市场的发展深度、广度和流动性。我们致力于促进亚洲资本市场的稳定、创新和竞争力，为区域经济的增长提供必要动力。我们针对关键问题，群策群力，统一立场，努力形成共识，寻求解决方案，并促成变革。我们多管齐下，包括与监管部门和交易所开展磋商，制定统一的行业标准，发表政策性专文呼吁深化市场发展，并降低亚太地区金融交易费用。通过与全球金融市场协会(GFMA)的另外两家分会，即位于美国的证券业和金融市场协会及位于欧洲的欧洲金融市场协会(AFME)合作，我们还积极推介全球最佳规范和标准，促进本区域发展。有关 ASIFMA 的更多信息载于：www.asifma.org.

第五十二条规定，中国证监会及其委托的第三方可以对核心机构和经营机构进行渗透测试和系统扫描。中国证监会《证券基金经营管理机构信息技术管理办法》第五十六条也规定了同样的要求。

我们理解，中国证监会希望通过独立测试，更好地评估核心机构和运营机构的网络安全计划及其防范优缺点。然而，若开展监管机构主导的或监管机构委托第三方主导的渗透测试，可能对企业和行业很不安全，因为渗透测试可能具有破坏性，且测试结果可能较为敏感，测试会给企业带来实际风险。在没有运营背景的情况下测试系统和应用程序，可能会对企业的运营造成重大干扰。测试只能在某个特定时间点就特定漏洞进行评估，只是企业成熟的“深度防范”办法中众多工具之一，只能评估风险情况和控制措施的效果，但无法为企业的整体安全状况提供全面的保证。

我们建议中国证监会重新考虑中国证监会现行《办法》第五十二条和《证券基金经营管理机构信息技术管理办法》第五十六条的做法，认可企业主导的渗透测试和漏洞扫描，允许企业有机会分享其漏洞管理方法，并与经营机构合作，确定经营机构可以证明其网络安全能力的其他方法。

监管信息技术服务提供商

我们注意到，《办法》草案中包含了一项建议，即在监管企业的同时，直接监管信息技术服务提供商的活动，这也是中国证监会《证券基金经营管理机构信息技术管理办法》中采取的监管方式。在全球范围内，信息技术服务提供商不受金融服务行业监管机构的许可或监管。金融监管机构要求受监管实体（即核心机构和经营机构）通过签订合同或其他方式，由委托的信息技术服务提供商负责提供适当的控制措施，履行报告义务，提供信息获取渠道。我们建议中国证监会与全球监管做法接轨，采取这种方式，而不是直接向信息技术服务提供商索取这些信息。这样，中国证监会将本着监管的精神，实现我们所理解的监管目标，同时保持被监管企业的合规义务。

全行业战略数据备份

我们注意到对全行业数据备份的要求。我们认为，核心机构和运营机构应按照全球标准和行业最佳管理负责自己的数据备份，不应依赖全行业的战略数据备份中心进行网络事件响应和恢复。

此外，如上文所强调的，共享数据存在重大风险——共享对企业网络安全敏感的数据尤其如此，因为这些数据对黑客和其他不法分子极为有用，并可能便于他们直接或通过供应链攻击经营机构和/或行业。

最后，部门范围内的战略数据备份中心给行业带来了集中风险，可能作为一站式宝贵数据库，而成为黑客和恶意分子攻击的目标。这不仅对所有核心机构和运营机构带来巨大的个体风险，而且鉴于全球金融业的相互联系，如果数据遭受破坏或泄露，还会给中国和全球金融业带来巨大的系统性风险。

因此，我们建议证监会鼓励企业通过使用国际标准和最佳做法，如金融行业网络安全框架（FSP或框架）[2]来提高自身的网络事件响应和恢复能力，并避免制造制造对整个行业有风险的单点故障。

基于风险和原则的方法

我们推荐中国证监会重点鼓励金融机构利用基于风险和原则的网络安全框架。这种框架可以适当地适用于所有金融市场参与者，无论其规模如何。全球金融业创建了“金融行业网络安全框架（“FSP或框架”），这是一款网络风险管理评估工具，可指导企业诊断网络风险，并应用相关标准和最佳做法来适当管理该风险。 “金融行业网络安全框架”采用了一种弹性的可扩展的分级机制，根据单个机构的风险和活动制定适合其自身情况的网络安全风险框架。框架根据机构的影响力分为四个层级：国家/超出国家影响、国家影响、行业影响、本地影响。例如，具有国家级或超出国家影响影响的第一级机构应根据277条诊断规定进行评估，而具有本地影响的第四级机构只需要根据137条诊断规定进行评估。“金融业概况”综合了业界最佳网络安全做法以及不同司法管辖区监管机构的要求。我们相信，证监会鼓励金融机构采用“金融行业网络安全框架”，并认可“金融行业网络安全框架”，有助于提高全球监管的协调性，提升行业的网络安全水平，并提高企业与证监会的沟通效率。若证监会能采取标准化的风险评估工具，就可以更好地识别行业的系统性风险，并有更多时间专注于着重需要监管注意力的事项。

除上述总体意见外，我们还就《办法》草案中的部分条款提交了具体的反馈意见，见下文。

我们真诚地希望中国证监会能积极考虑我们的建议。如果您有任何问题，我们会及时回复，并欢迎能举行线上会议，进行深入讨论。

顺颂时祺！

亚洲证券业与金融市场协会技术和运营执行董事

Laurence Van der Loo

具体条款修订意见：

具体条款	条款内容	ASIFMA 反馈意见
第七条	中国证券业协会、中国期货业协会、中国证券投资基金业协会等行业协会（以下统称行业协会）依法制定行业网络安全自律规则，对经营机构网络安全实施自律管理。	• 我们建议，自律规则的制定应遵循透明、公开、公正、共识、有效、相关、一致的原则。我们希望与中国证监会确认，经营机构可以自愿参加行业协会的自律管理项目。我们建议将第七条内容修订如下：“中国证券业协会、中国期货业协会、中国证券投资基金业协会等行业协会（以下统称行业协会）可以本着透明、公开、公正、共识、有效、相关、一致的原则，依法制定行业网络安全自律规则，经营机构可自愿加入行业自律计划。行业协会可对参与计划的经营机构网络安全实施自律管理。”
第十三条	核心机构和经营机构应当确保信息系统和相关基础设施具备合理的架构，足够的性能、容量、可靠性、扩展性和安全性，并保证相关安全技术措施与信息化工作同步规划、同步建设、同步使用。信息系统的性能容量不得低于历史峰值的两倍。	• 关键术语“性能容量”界定不明。是指整个系统的容量，还是单一容量指标，如CPU、磁盘等？“历史峰值”的数值可能是动态的。我们请证监会阐明：这是否意味着需要非常频繁地调整性能容量，以确保始终不低于历史峰值的两倍。如果是这样，企业不断调整或扩大性能容量要求会非常困难。 • 我们建议《办法》草案与证监会《信息技术管理办法》中的要求保持一致，重点关注重要信息系统，采取基于风险和原则的方法，不对技术性能作出规定。中国证监会《证券基金经营管理机构信息技术管理办法》第二十三条指出：“证券基金经营机构应当结合公司发展战略、市场交易规模等因素定期对重要信息系统开展压力测试和评估分析，确保其容量满足业务开展需要。”我们建议修订《办法》草案第十三条的内容，与证监会《证券基金经营管理机构信息技术管理办法》的要求保持一致：“第十三条：核心机构和经营机构应当确保信息系统及相关基础设施结构合理、性能充分、容量大、可靠性强、可扩展性好、安全性高，并确保相关安全技术措施与信息化工作同步规划、同步建设、

		同步使用。核心机构和经营机构应确保重要信息系统的容量满足业务开展需要。~~信息系统的性能容量不得低于历史峰值的两倍。~~
第十五条	核心机构和经营机构新建上线、运行变更、下线移除重要信息系统的，应当进行风险评估并开展充分测试，制定应急处置和回退方案；可能对证券期货市场安全平稳运行产生较大影响的，应当提前向中国证监会及其派出机构报告。	• 我们建议与现有要求保持一致，希望《办法》草案与中国证监会《证券基金经营管理机构信息技术管理办法》中的变更管理通知要求保持一致，在新建、置换重要信息系统所在机房，或与证券、基金交易有关的信息系统时，证券、基金公司应在相关业务活动前 5 个工作日内向中国证监会提交相关材料，包括内部审查意见、机房基本情况、技术架构设计、操作流程、信息安全管理材料、业务制度、合规管理、风险管理制度等。
第十七条	核心机构和经营机构应当建立健全网络安全监测预警机制，设定监测指标，持续监测信息系统和相关基础设施的运行状况，及时处置异常情形，对监测机制执行效果进行定期评估并持续优化。 核心机构和经营机构应当全面、准确记录并妥善保存生产运营过程中的业务日志和系统日志，确保满足故障分析、内部控制、调查取证等工作的需要。业务日志保存期限不得少于二十年，系统日志保存期限不得少于六个月。	• 要求“业务日志保存期限不得少于二十年”可能较为苛刻，我们希望中国证监会能够分享这一要求背后的考虑。 • 《证券法》（2019年）[3]对客户的开户材料、委托记录、交易记录以及与内部管理和业务操作有关的所有信息提出了全面的保存要求。我们建议《办法》草案与《证券法》中的范围保持一致，并删除未加定义的“业务日志”一词。
第十八条	核心机构和经营机构应当建立同城和异地数据备份设施，至少每天备份数据一次，每季度至	• 中国证监会《证券基金经营管理机构信息技术管理办法》全面规定了数据备份要求，并提出了中国证监会在这方面的期

3

	少对数据备份进行一次有效性验证。核心机构和经营机构应当建立信息系统的故障备份设施和灾难备份设施，根据信息系统的重要程度和影响范围，确定恢复目标，保证业务活动连续。灾难备份设施应当通过同城或者异地灾难备份中心的形式体现。核心机构和经营机构采取双活或者多活架构部署重要信息系统的，确保业务连续运行能力不低于前款规定的前提下，任一数据中心可以视为其他数据中心的灾难备份设施。	望。我们希望确认：《办法》草案中的要求与《证券基金经营管理机构信息技术管理办法》中的数据备份要求是一致的。并建议《办法》草案在措辞和方法上与《证券基金经营管理机构信息技术管理办法》保持一致，以减少混淆和误解。
第十九条	核心机构和经营机构应当至少每半年开展一次重要信息系统压力测试，根据系统技术特点和承载业务类型，制定压力测试方案，设定测试场景，设定测试场景，从系统处理能力、网络冗余、灾备建设等方面设置测试指标，有序组织测试工作，测试完成后形成压力测试报告存档备查。 核心机构和经营机构应当按照有关要求，参加中国证监会组织开展的全行业重要信息系统压力测试，并根据测试情况及时整改；暂时无法整改的，应当制定切实可行的整改计划。	• 我们建议全球金融机构可以利用并依托现有的全球或区域测试。 • 本条要求对重要系统进行压力测试。我们希望中国证监会阐明压力测试的要求，并说明“重要信息系统”的定义是否与中国证监会《证券基金经营管理机构信息技术管理办法》中的一致。 • 我们建议，《办法》草案与中国证监会《证券基金经营管理机构信息技术管理办法》中的要求保持一致，并采取基于风险和原则的方法，不对技术性能作出硬性规定。中国证监会《信息技术管理办法》第二十三条指出：“证券基金经营机构应当结合公司发展战略、市场交易规模等因素定期对重要信息系统开展压力测试和评估分析，确保其容量满足业务开展需要。”我们建议修订《办法》草案第十九条，与中国证监会《信息技术管理办法》的规定保持一致：“第十九条：核心机构和经营机构应当定期开展一次重要信息系统压力测试，根据系统技术特点和承载业务类型，制定压力测试方案，设定测试场景，”从系统处理能力、网络冗余、灾备

		建设等方面设置测试指标，有序组织测试工作，测试完成后形成压力测试报告存档备查。”
第二十条	信息技术服务机构应当依法向中国证监会备案，并按照有关业务规则为证券期货业务活动提供信息技术产品或者服务。核心机构和经营机构应当建立健全内部管理机制，完善信息技术产品和服务准入标准，审慎采购并持续评估相关产品和服务的质量，加强保密管理，及时改进风险管理措施，健全应急处置机制，保障本机构网络安全和相关业务的安全平稳运行。	• 正如在总体意见部分所强调的，我们建议中国证监会与全球普遍做法接轨，即要求受监管实体（即核心机构和经营机构）通过签订合同或其他方式，由信息技术服务提供商负责提供适当的控制措施，履行报告义务，提供信息获取渠道。
第二十一条	核心机构和经营机构应当加强自主研发能力建设，持续提升自主可控能力，并按照国家及中国证监会有关要求开展信息技术应用创新相关工作。	• 我们请中国证监会阐明，“自主可控能力”是指内部开发与外包的区别，还是应该从更广泛的角度理解？ • 我们建议《办法》草案采用技术中立方式，允许企业灵活选择最适合其业务和运营需求的技术。
第二十三条	(5)构建数据质量评估框架，建立质量管控和追责机制。	• 第(5)款提到了构建数据质量评估框架，建立质量管控和追责机制。我们请证监会阐明数据质量评估框架，例如这种框架和机制的最佳参考做法。
第二十四条	核心机构和经营机构处理重要数据、核心数据的，应当依法明确数据安全负责人，指定数据安全管理机构或者部门。核心机构和经营机构处理重要数据的信息系统原则上应当满足三级以上网络安全等级保护要求，处理核心数据的	• 第二十四条规定，处理重要数据的系统应满足多级保护计划三级以上要求。这是否意味着系统可以被归类为二级，但满足三级要求？ • 《网络安全等级保护条例》（2018 年草案）确立了多级保护分类的标准和流程，在涉及多级保护分类时，应将其作为权威指导。我们建议证监会在分类标准上参考《网络安全等级保护条例》草案，删除关于“重要数据”的附加标准，以保持规则的一致性。我们建议修订第二十四条的内

	信息系统依照有关法律法规从严保护。	容，如下：“第二十四条：核心机构和经营机构处理重要数据、核心数据的，应当依法明确数据安全负责人，指定数据安全管理机构或者部门。处理核心数据的信息系统应根据相关法律和法规受到严格保护。”
第二十六条	核心机构和经营机构应当遵循合法、正当、必要和诚信原则处理投资者个人信息，依法履行投资者个人信息保护义务。	• 我们建议在措辞上与《个人信息保护法》保持一致。“监管要求”一词过于宽泛，因此可能会扩大《个人信息保护法》规定的情况，在实践中可能会造成一些不确定性。 • 因此，我们建议将此条改为：“为履行法定职责、法定义务~~或者监管要求所必需~~，核心机构和经营机构可以在未取得个人同意的情况下，处理个人信息”。 •
第二十九条	中国证监会可以指定相关机构建设证券期货业战略备份数据中心，开展行业数据的集中备份和管理工作，持续提升证券期货业重大灾难应对能力。核心机构和经营机构应当按照规定及时向证券期货业战略数据备份中心报送数据，报送的数据必须真实、准确、完整。	• 我们建议，应允许全球金融机构在全球或地区范围内利用现有的备份数据中心。 • 正如总体意见部分所强调的，我们建议：核心机构和经营机构应负责按照全球标准和行业最佳做法开展数据备份，而不应该依赖全行业的战略数据备份中心，进行网络事件响应和恢复。此外，正如总体意见部分所强调的那样，共享数据存在着巨大的风险，特别是对公司网络安全敏感的数据，因为这些数据对黑客和其他不法分子极为有用，并可能便于他们直接或通过供应链攻击经营机构和/或行业。因此，我们希望与中国证监会合作，尽量减少数据收集，减少电子足迹，如果出于监管目的绝对需要敏感数据，则寻求其他途径。最后，部门范围内的战略数据备份中心给行业带来了集中风险，可能作为一站式宝贵数据库，成为黑客和恶意分子攻击的目标。这不仅对所有核心机构和运营机构带来巨大的个体风险，而且由于全球金融业相互联系，如果数据遭到破坏或泄露，还会给中国和全球金融业带来巨大的系统性风险。因此，我们建议证监会鼓励企业采取国际标准和最佳做法（如《金融行业网络安全框架》），来提高自身的网络事件

		响应和恢复能力，并避免造成对整个行业带来风险对单点故障。
第四章	**网络安全应急处置**	• 我们建议《办法》草案与中国证监会 2021 年《证券期货业网络安全事件报告与调查处理办法》中关于处理网络安全事件的相关要求保持一致。
第三十条	核心机构和经营机构应当建立网络安全风险监测预警机制，加强日常监测，定期开展漏洞扫描、安全评估等工作。 核心机构、经营机构和信息技术服务机构发现网络安全产品或者服务存在安全缺陷、系统漏洞等风险隐患的，应当及时核实并加固整改；可能对证券期货业网络安全产生较大影响的，应当向中国证监会及其派出机构报告。 中国证监会及其派出机构可以就相关安全缺陷、系统漏洞等风险隐患开展行业通报，核心机构、经营机构和信息技术服务机构应当及时排查并采取风险防范措施。	• 我们建议，应允许全球金融机构利用并依托在全球或区域范围内执行的现有风险监测和漏洞扫描程序。
第四十一条	证券期货业关基单位应当对关键信息基础设施的安全运行进行持续监测，定期开展压力测试，发现系统性能和网络容量不足的，应当及时采取系统升级、扩容等处置措施，确保系统性能容量不低于历史峰值的三倍，网络带宽不得低于历史峰值的两倍。	• “历史峰值”的数值可能是动态的。 我们请中国证监会阐明：这是否意味着关基单位需要非常频繁地调整性能容量，以确保始终不低于历史峰值的两三倍？ 如果是这样，企业不断调整或扩大性能容量要求会非常困难。

第四十六条	核心机构可以申请国家专业资质，开展证券期货业网络安全认证、检测、测试和风险评估等工作。相关核心机构应当保障充足的资源投入，完善内部管理制度和工作流程，保证工作专业性、独立性和公信力。中国证监会定期对核心机构前款工作开展情况开展评估，评估通过的，可以将其作为证券期货业网络安全监管支撑单位，相关工作开展情况可以作为中国证监会及其派出机构实施监督管理的参考依据。	• 我们赞赏中国证监会支持核心机构及其分支机构运用网络安全国家专业资质开展证券期货业网络安全检测、认证、评估等网络安全监管工作。我们希望确认：企业也可以委托具有相应网络安全资质的国家实体进行网络安全认证、评估和检测。
第四十九条	行业协会应当鼓励、引导网络安全技术创新与应用，增强自主可控能力，组织开展科技奖励，促进行业科技进步。行业协会应当引导信息技术服务机构规范参与行业网络安全和信息化工作，促进市场公平竞争。	• 我们建议《办法》草案采用技术中立原则，允许企业灵活选择最适合其业务和运营需要的技术。
第五十条	中国证监会及其派出机构可以要求核心机构、经营机构和信息技术服务机构提供证券期货业网络安全管理相关信息和数据。相关机构应当配合，及时、准确、完整提供相关资料。	• 正如总体意见部分所强调的，我们希望与中国证监会合作，确保所要求的网络安全相关数据并非敏感数据，而且以安全、可靠的方式处理数据。如果出于监管目的，要求必须提供敏感数据，我们鼓励中国证监会尽量减少电子数据的收集，并探索其他方法，如由监管机构前往企业经营场地查看数据，以降低风险。我们建议将第五十条内容修订如下：“为了履行本《办法》规定的职责，中国证监会及其派出机构根据法律和法规规定，可以要求核心机构、经营机构和信息技术服务机构及时提供证券期货业网络安全管理相关材料，且提供的材料必须真实、准确、完整”。

第五十二条	中国证监会及其派出机构可以委托国家、行业有关专业机构采用渗透测试、漏洞扫描及信息技术风险评估等方式，协助对核心机构、经营机构和信息技术服务机构开展监督、检查。	• 我们强烈建议删除第五十二条。 • 我们理解，中国证监会希望通过独立测试，更好地评估核心机构和运营机构的网络安全计划及其防范优缺点。然而，若开展渗透测试，可能对企业和行业不安全，因为渗透测试可能具有破坏性，且测试结果可能较为敏感，测试会给企业带来实际风险。在没有运营背景的情况下测试系统和应用程序，可能会对企业的运营造成重大干扰。测试只能在某个特定时间点就特定漏洞进行评估。 无论测试多么广泛、多么复杂，也只是企业成熟的“深度防范”办法中众多工具之一，只能评估风险情况，和控制措施的效果， 但无法为企业的整体安全状况提供全面的保证。我们建议中国证监会承认企业主导的渗透测试和漏洞扫描，并与经营机构合作，确定可以证明其网络安全能力的其他方法。 • 我们还建议，应允许金融机构利用并依托现有的全球或区域性内部渗透测试。
第六十二条	(5) 重要数据、核心数据，是指按照《数据安全法》、国家和证券期货业有关数据分类分级保护制度，确定的重要数据、核心数据。	• 第 5 款指出，数据、核心数据，是指《数据安全法》、国家和证券期货业有关数据分类分级保护制度定义的重要数据、核心数据。目前，关键术语的定义和范围以及数据分类工作仍不明确。 我们建议中国证监会在起草数据分类指南或界定“重要数据”或“核心数据 ”等关键术语的范围时，与业界进行磋商，并确保起草过程公开、透明、包容。