《证券期货业网络安全管理办法（征求意见稿）》起草说明

为建立健全证券期货业网络安全监管制度体系，防范化解行业网络安全风险隐患，维护资本市场安全平稳高效运行，在充分衔接上位要求、总结监管实践的基础上，证监会研究起草了《证券期货业网络安全管理办法（征求意见稿）》（以下简称《办法》）。现说明如下：

一、起草背景

近年来，证券期货业机构对网络安全的重视程度大幅提升，组织架构和制度体系持续优化，信息技术投入逐年增加，行业网络安全运行态势总体平稳。但是，随着行业数字化加速发展、网络安全上升为国家战略、资本市场持续深化改革等内外部条件的变化，证券期货业网络安全面临的新情况新问题逐渐凸显，主要体现在以下方面：

（一）行业网络安全形势严峻复杂。一是随着大数据、云计算、区块链和人工智能等新技术应用的不断深入，证券期货业务与技术加速融合，各类业务活动日益依赖网络安全和信息化，增加了网络安全管理的复杂度。二是随着行业机构数字化转型的提速，信息系统建设任务明显增加，上线变更操作较为频繁，行业网络安全管理能力面临更大挑战。

（二）法律法规的上位要求有待进一步落实。《网络安

全法》于2017年6月正式施行，2021年下半年以来，《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规密集发布实施，我国网络安全法律体系进一步健全，新型网络安全管理框架基本成型。对此，证监会虽于2012年以来发布《证券期货业信息安全保障管理办法》(证监会令82号)《证券基金经营机构信息技术管理办法》（证监会令152号）等监管规则，但是由于制定时间较早、监管实践变化等原因，相关监管规则在有效衔接上位要求方面有待进一步完善。

（三）监管实践成果制度化还需加强。2020年以来，证监会稳步推动科技监管深化改革，监管体制机制不断优化，信息技术服务机构备案管理、资本市场金融科技创新试点等工作全面展开，与相关部委进一步形成监管合力，沟通协作更加顺畅，需要及时总结实践经验，将改革成果制度化机制化。

基于上述新情况新问题，亟需进一步健全证券期货业网络安全监管制度体系，制定专门的行业网络安全管理相关的部门规章，补齐制度供给短板，构建证券期货业网络安全管理的体系框架，提升行业网络安全保障能力。

二、起草思路

（一）落实上位要求，汲取实践经验。《办法》聚焦网络安全管理，强化数据安全和个人信息保护，结合证券期货

业特点，为《网络安全法》《关键信息基础设施安全保护条例》等法律法规在证券期货业的有效落地，明确实施路径，提供制度保障。同时，总结行业近年来监管工作成效，将实践经验转化为制度成果，固化工作机制。

（二）覆盖各类主体，厘清权责边界。一方面，充分考虑证券期货业各类主体的责任义务和业务特点，对证券期货业关键信息基础设施运营单位、核心机构、经营机构以及信息技术服务机构，从网络安全管理方面分别提出监管要求。另一方面，理清职责分工，对各方监管部门、自律组织的网络安全监管职责做出明确规定。

（三）严守安全底线，促进科技发展。《办法》以保障安全为基本原则，从建设、运维、使用网络及信息系统，到识别、监测、防范、处置风险等方面，构建了完整的网络安全监管框架，对行业机构提出全方位的网络安全管理要求。在此基础上，《办法》还注重通过发展解决问题，通过技术架构的升级优化，提升安全保障能力，并在信息基础设施建设、金融科技创新等方面做出了制度安排。

三、主要内容

《办法》共八章六十六条，对证券期货业网络安全监督管理体系、网络安全运行、数据安全统筹管理、网络安全应急处置、关键信息基础设施网络安全、网络安全促进与发展、监督管理与法律责任等方面提出了要求。具体包括：

（一）总则。规定立法宗旨、适用范围、适用主体、工作目标及监管职责，厘清核心机构、经营机构和信息技术服务机构等行业机构的责任边界。

（二）网络安全运行。督促行业机构建立健全网络安全管理体制机制，提升网络安全运行保障能力。一是要求核心机构、经营机构具有完善的治理架构，强化管理层责任，指定牵头部门，保障资源投入。二是对核心机构、经营机构的信息系统和相关基础设施提出基本要求，明确等级保护义务。三是要求核心机构、经营机构审慎开展系统新建、变更和移除，及时履行投资者告知义务，加强日常监测。四是对核心机构、经营机构明确信息系统备份能力有关要求，提出压力测试常态化要求。五是从制度体系、人员配备、合规安全等方面，对信息技术服务机构提出监管要求。六是强化核心机构、经营机构采购产品和服务的准入、评估、改进要求，提升自主研发和安全可控能力，加强知识产权保护。

（三）数据安全统筹管理。一是从制度机制、组织架构、行业数据标准、权限管理、质量评估、防范泄露损毁等方面，明确证券期货业的具体要求。二是配套上位要求，对数据分类分级、个人信息保护、规范信息发布等方面作进一步强调。三是为建立证券期货业战略备份数据中心预留制度空间，提升行业极限灾难应对能力。

（四）网络安全应急处置。一是建立风险监测预警体制，

加强日常漏洞扫描、安全评估，及时消除风险隐患。二是完善应急预案的应急场景和处置流程，要求定期开展应急演练。三是强化网络安全事件报告和调查处理工作，明确故障排查、相关方告知等工作要求。

（五）关键信息基础设施网络安全。落实国家关于关键信息基础设施的安全保护要求，结合行业特点，从组织保障、建设评审、变化报告、检测评估、采购管理、性能容量、灾难备份等方面，对关键信息基础设施运营单位提出进一步的督导要求。

（六）网络安全促进与发展。一是鼓励相关机构在依法合规、风险可控、不损害投资者利益的前提下，开展行业网络安全技术应用。二是核心机构、经营机构可以在保障自身信息系统安全的前提下，为行业提供信息基础设施服务。三是建立金融科技创新监管机制，加强网络安全监管专业支撑，核心机构可以申请国家相关专业资质，开展行业网络安全认证、检测、测试和风险评估等工作。四是强化行业网络安全人才队伍建设，定期开展网络安全宣传与教育。五是发挥行业协会作用，引导网络安全技术创新与应用，组织科技奖励，促进行业科技进步、市场公平竞争。

（七）监督管理与法律责任。一是规定行业机构的报告义务和流程要求。二是明确证监会及其派出机构可以委托专业机构采用渗透测试、漏洞扫描和风险评估等方式对行业机

构开展监督检查。三是对重要时期的网络安全保障工作明确制度安排。四是依据上位要求，结合违法违规的具体情形，规定相应罚则，并规定创新容错相关制度安排。

此外，《办法》还明确了名词释义、参照执行主体和情境、实施时间以及相关办法衔接等事项。