《证券期货业网络和信息安全管理办法》立法说明

为建立健全证券期货业网络和信息安全监管制度体系，防范化解行业网络和信息安全风险隐患，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，证监会起草了《证券期货业网络和信息安全管理办法》（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和信息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，行业网络和信息安全运行态势总体平稳。但是，随着行业数字化智能化加速发展、网络和信息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，证券期货业网络和信息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）行业网络和信息安全形势严峻复杂。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，增加了网络和信息安全管理的复杂度。二是随着行业机构数字化智能化转型的提速，信息系统建设任务明显增加，上线变更操作较为频繁，行业网络和信息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。随着《网络安全法》《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，我国网络和信息安全法律体系进一步健全，新型管理框架基本成型。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，信息技术系统服务机构备案管理、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，有必要进一步健全证券期货业网络和信息安全监管制度体系，制定专门的部门规章，构建证券期货业网络和信息安全管理的体系框架，提升行业安全保障能力。

二、起草思路

（一）落实上位要求，汲取实践经验。《办法》聚焦网络和信息安全管理，强化个人信息保护，结合证券期货业特点，为相关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者、核心机构、经营机构以及信息技术系统服务机构，从网络和信息安全管理方面分别提出监管要求。另一方面，厘清职责分工，对监管部门、自律组织的网络和信息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，构建了完整的网络和信息安全监管框架，对行业机构提出全方位的管理要求。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作出制度安排。

三、主要内容

《办法》共八章七十五条，对证券期货业网络和信息安全监督管理体系、网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展、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系统服务机构等行业机构的责任边界。

（二）网络和信息安全运行。督促行业机构建立健全网

络和信息安全管理体制机制，提升安全运行保障能力。**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，指定或设立牵头部门，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，充分评估技术和业务风险，保证充分测试，及时履行投资者告知义务，加强网络和信息安全日常监测。**四是**要求核心机构、经营机构建立网络和信息安全防护体系，明确数据备份、信息系统备份有关要求，常态化开展压力测试。**五是**强化核心机构、经营机构对供应商的管理，督促信息技术系统服务机构履行备案义务，提升自主研发和安全可控能力，加强知识产权保护。**六是**明确安全信息发布和行业数据备份中心相关要求。

（三）投资者个人信息保护。**一是**明确核心机构和经营机构处理投资者个人信息的基本原则，要求建立健全投资者个人信息保护体系和管理机制，履行保护义务。**二是**明确核心机构和经营机构在投资者个人信息处理、共享环节的安全防护要求。**三是**提出核心机构和经营机构在网络安全防护边界外处理投资者个人信息的技术要求，防范化解信息泄露风险。**四是**对核心机构和经营机构收集客户生物特征的必要性和安全性提出评估要求。

（四）网络和信息安全应急处置。**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）关键信息基础设施安全保护。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、监测评估、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者提出进一步的督导要求。

（六）网络和信息安全促进与发展。**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，开展行业网络和信息安全技术应用。**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，加强网络和信息安全监管专业支撑，核心机构可以申请国家相关专业资质，开展行业网络和信息安全相关认证、检测、测试和风险评估等工作。**四是**强化行业人才队伍建设，定期开展网络和信息安全宣传与教育。**五是**发挥行业协会作用，引导技术创新与应用，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**建立健全行业网络和信息安全态势感知工作机制，开展风险隐患行业通报。**三是**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。**四是**对重要时期的网络和信息安全保障工作明确制度安排。**五是**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。《办法》施行后，证监会此前发布的《证券期货业信息安全保障管理办法》同时废止。

四、公开征求意见情况

公开征求意见阶段，各方对《办法》表示充分认可，一致认为《办法》的制定，有利于完善证券期货业网络和信息安全制度体系，提升行业安全平稳运行保障水平。我们充分吸收采纳了合理意见。未采纳的意见主要是操作层面和文字表述意见，还有一些意见涉及的事项不属于《办法》规制范围，或者相关法律法规、规章已有规定，因此未予采纳。