《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》起草说明

2012 年 12 月，我会印发了《证券期货业信息安全事件报告与调查处理办法》（证监会公告〔2012〕46 号）。总体来看，《证券期货业信息安全事件报告与调查处理办法》在规范证券期货业网络安全事件的报告和调查处理工作，减少网络安全事件的发生，维护投资者合法权益和资本市场稳定方面，发挥了积极的作用。但是，经过近几年的实践，逐渐发现《证券期货业信息安全事件报告与调查处理办法》在信息系统分类、网络安全事件分级、责任追究、事件处置等方面需要进一步完善。

为进一步规范证券期货业网络安全事件报告和责任追究，依据《证券法》《证券投资基金法》《期货交易管理条例》《证券期货业信息安全保障管理办法》（证监会第 82 号令）《证券基金经营机构信息技术管理办法》（证监会第 152 号令）等法律法规和证监会规章，我会开展了《证券期货业信息安全事件报告与调查处理办法》修订工作，形成了《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》。现将有关情况说明如下:

一、修订背景

《证券期货业信息安全事件报告与调查处理办法》对证券期货业网络安全事件应急和调查处理提出了要求，规定了行业机构和监管部门调查处理网络安全事件的基本权利和义务，固化了证券期货业网络安全事件报告、调查处理机制，但也存在以下需进一步完善之处:

一是未对证券期货业信息系统进行统一分类。《办法》仅列举了部分重要系统，而未依据信息系统的重要性进行统一分类，在实际工作中存在未列举信息系统发生网络安全事件，无法依据《办法》确定信息系统类别及其重要性的情况，导致不能对部分网络安全事件进行合理定级。

二是未定量描述事件级别。《办法》通过“全部中断”、“部分中断”等用语来描述事件的严重程度，但如何界定全部中断、部分中断，在实际操作中存在较大的主观性，不利于客观判定事件的影响情况。

三是事件报告效率较低。《办法》规定应急报告时先进行电话报告，随后书面报送《信息安全事件情况报告书》，未考虑通过更加高效的平台报告事件；事件报告未初步评估事件级别，不利于采取针对性的措施；只要求严重故障立即报告，一般故障 30 分钟无法恢复的才需要报告，而现实场景很难判断故障是否会持续升级，从而导致事件迟报。

四是处罚缺乏针对性和灵活性。《办法》未区分信息系统用户数量、网络安全事件是否造成重大影响、信息系统是

否已按标准或最佳实践建设，笼统的将所有事件定为网络安全事件，灵活性不足。

二、起草思路

此次修订主要包括以下内容:

（一）对规范范围进行了界定

一是进一步明确了责任主体。《证券期货业信息安全保障管理办法》（证监会第 82 号令）规定的责任主体是：“承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其下属机构（以下简称核心机构）；证券公司、期货公司、基金管理公司、证券期货服务机构等证券期货经营机构（以下简称经营机构）。”此次起草工作将责任主体进一步明确为：“承担证券期货市场公共职能的机构、承担证券期货行业信息技术公共基础设施运营的机构等证券期货市场核心机构及其**承担上述公共职能的**下属机构（以下简称核心机构），证券公司、期货公司、基金管理公司**及其提供证券期货相关服务的下属机构**、证券期货服务机构等证券期货经营机构（以下简称经营机构）”。

二是明确了对证券期货服务机构采取监督管理措施。根据《证券法》《证券投资基金法》《证券期货业信息安全保障管理办法》（证监会第 82 号令）《证券基金经营机构信息技术管理办法》（证监会第 152 号令）等法律法规和证监

会规章，将证券期货服务机构明确为证券期货业网络安全保障责任主体，网络安全事件相关证券期货服务机构存在人为责任的，中国证监会及其派出机构可以要求其提交说明材料，并依照有关法律、行政法规和规章，采取监督管理措施。

（二）与相关法律法规使用相同的用语

为与《网络安全法》等法律法规的表述保持一致，此次起草工作将《证券期货业信息安全事件报告与调查处理办法》改为《证券期货业网络安全事件报告与调查处理办法》，对文件中相关内容也进行了规范统一。

（三）对信息系统进行了统一分类

按照信息系统发生网络安全事件后，对国家金融安全、社会秩序、投资者合法权益造成的损害程度，核心机构和经营机构的信息系统由高到低分为五类，即五类系统、四类系统、三类系统、二类系统和一类系统。

对于未列在典型系统/模块表中的信息系统，如果发生网络安全事件，应首先依据分类原则进行分类，以确定信息系统的重要性。

（四）增加了定量描述系统服务能力异常的方法

信息系统服务能力异常分为严重异常、中度异常和轻度异常。其中，严重异常是指信息系统发生故障，服务能力异常 80%以上的情形；中度异常是指信息系统发生故障，服务能力异常 30%以上且未构成严重异常的情形；轻度异常是指

信息系统发生故障，服务能力异常但未构成严重异常、中度异常的情形。为便于实际操作，具体给出了证券期货交易类信息系统、证券交易场所交易基金销售类信息系统、基金销售及会计核算或者注册登记系统、行情计算发布类信息系统、开户类信息系统、网站类信息系统、行业基础通信系统等典型系统的服务能力异常计算方法。

（五）给出了统一的网络安全事件分级方法

网络安全事件分为特别重大事件、重大事件、较大事件和一般事件。结合信息系统类别、信息系统服务能力下降程度和网络安全事件持续时间，给出了统一的网络安全事件分级标准。同时，对于数据泄露、结算金额差错、发布不良信息等网络安全事件，依据数据量和影响程度等给出了定级标准。

考虑到结算系统等中后台业务系统发生网络安全事件后，其对市场的影响是通过交易行情系统等前台系统表现出来，因此依据受影响的前台系统对结算系统事件进行定级。

（六）完善优化了网络安全事件报告流程

一是为进一步提高网络安全事件报告处置的及时性和系统性，本次起草工作增加了通过事件报送平台报告事件情况。二是考虑到事件发生时，很难判断是否会进一步恶化，要求信息系统发生故障，可能构成网络安全事件的，都应当立即报告。三是为提高应急处置效率，要求机构对事件初步

定级，对可能构成特别重大、重大网络安全事件的，每隔30分钟至少上报一次事件处置情况，直至信息系统恢复正常运行；对较大和一般网络安全事件，第一次上报后，无须持续上报事件处置情况；如有重要情况应当立即报告。

（七）处罚更加具有针对性和灵活性

一是对于社会影响较大且存在明显过错的网络安全事件，可酌情提高事件定级；二是从鼓励行业自主创新、网络安全事件实际影响、尽职免责等角度出发，对未发现明显过错、疏忽且不良影响较小的网络安全事件，可酌情从轻分级或不认定为网络安全事件：1、自主研发的信息系统上线一年内发生网络安全事件的；2、基金销售、会计核算、注册登记系统发生网络安全事件后及时修复，未对行业及投资者权益造成影响的；3、具有冗余架构的信息系统或基础设施，在合理的切换时间内不影响系统提供正常服务的；4、经营机构面向50名以下投资者提供服务或者网络安全事件发生前一个月日均成交笔数不足50笔的信息系统、分支机构信息系统发生故障，处置得当，受影响客户得到妥善安抚的。

（八）关于结算系统等中后台业务系统故障的考虑

一般而言，结算系统等中后台业务系统的实时性不强，如果中后台业务系统发生故障，投资者将通过受其影响的交易行情等前台业务系统、投资者数据和结算金额差错、直接资金损失等感受到。因此，《征求意见稿》未对结算系统进

行分类，也未依据结算系统故障时间进行事件分级，而是按照受其影响的前台业务系统的类别和受影响程度，或按照其导致的投资者数据和结算金额差错、直接资金损失等，进行结算系统等中后台业务系统网络安全事件的分类分级。

三、主要内容

《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》共分五章，三十二条。分别是“总则”、“事件分类分级”、“事件报告”、“调查处理”和“附则”。

（一）总则

规定了《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》的制定目的、依据、适用范围，以及网络安全事件报告和调查处理原则。

（二）事件分类分级

《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》依据网络安全事件对投资者合法权益或资本市场造成影响的程度，将证券期货业信息系统分为 5 类，同时，根据网络安全事件影响程度，分为特别重大事件、重大事件、较大事件和一般事件 4 级。

（三）事件报告

《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》对有关网络安全事件的报告划分为 3 种情况：预警事件报告、网络安全事件应急报告、事后总结报告，并分

别明确了报告时限、报告路径和报告内容的要求。

（四）调查处理

规定了调查主客体的权利和义务，确保调查处理工作的顺利进行。明确了以下处罚措施：一是核心机构、经营机构在研发、测试、上线及运维等系统管理过程中未能严格执行相关法律法规和行业相关技术管理规定、技术规则、技术指引和技术标准，造成网络安全事件的，中国证监会及其派出机构依照有关法律、行政法规和规章，对发生网络安全事件的机构及相关负责人员采取监督管理措施或者实施行政处罚。二是发生网络安全事件的机构，妨碍网络安全事件报告与调查处理的，中国证监会或者其派出机构依照有关法律、行政法规和规章，对其采取监督管理措施或者实施行政处罚。

（五）附则

说明了《证券期货业网络安全事件报告与调查处理办法（征求意见稿）》的施行时间。