《证券期货业网络安全事件报告与调查处理办法》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）。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》。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。经过较长时间的实践，我们逐渐发现《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。

二、主要内容

《证券期货业网络安全事件报告与调查处理办法》共分五章，三十条。分别是“总则”、“事件分类分级”、“事件报告”、 “调查处理”和“附则”。 主要内容如下:

（一）进一步明确责任主体

一是将责任主体进一步明确为:“包括证券期货交易场所、证券登记结算机构等承担证券期货市场公共职能、承担证券期货业信息技术公共基础设施运营的证券期货市场核心机构及其承担上述相关职能的下属机构（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）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。

（三）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系统、证券交易场所交易基金销售类系统、基金销售及会计核算或者注册登记系统、行情计算发布类系统、开户类系统、网站类系统、行业基础通信系统等典型系统的服务能力异常计算方法。

（四）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、发布违法和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。

（五）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，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。

（六）处罚更加具有针对性和严肃性

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。