《中国人民银行业务领域网络安全事件报告管理办法（征求意见稿）》起草说明

2002年，中国人民银行制定印发《银行计算机安全事件报告管理制度》（银发〔2002〕280号，以下简称《现行制度》），明确了银行机构向中国人民银行报告计算机安全事件的管理要求。为应对网络安全新形势，进一步规范中国人民银行业务领域网络安全事件报告管理，更好地保障金融服务与维护金融安全，中国人民银行拟废止《现行制度》，并起草《中国人民银行业务领域网络安全事件报告管理办法（征求意见稿）》（以下简称《办法》）。现将相关情况说明如下:

一、制定必要性

（一）落实衔接法律法规要求。随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律、行政法规相继出台，按照规定向有关主管部门报告网络安全事件，已成为金融从业机构基本法定义务。为全面落实、有机衔接法律法规，需重新编写制度，在中国人民银行职责范围内进一步明确相关金融从业机构报告网络安全事件的具体要求。

（二）加强网络安全事件分级管理。科学合理判定网络安全事件级别是规范网络安全事件报告处置、开展网络安全

事件调查分析和责任认定的基础。《现行制度》仅简单列举“严重威胁银行资金安全”等网络安全事件报告的触发条件，未明确网络安全事件分级具体要求和底线规则，不符合《国家网络安全事件应急预案》等规定对网络安全事件实施分级管理的要求，因此需重新编写制度，规范金融从业机构针对中国人民银行业务领域网络安全事件的定级行为。

（三）规范网络安全事件报告要求。《现行制度》未明确网络安全事件事发、事中、事后报告要求，不适用于银行机构以外的其他金融从业机构。部分网络安全事件发生后，中国人民银行无法及时获悉事件应对处置情况和调查分析结果，也无法准确掌握中国人民银行业务领域网络安全总体态势，因此需重新编写制度，明确网络安全事件报告责任主体、内容、流程、时效等具体要求，指导监督金融从业机构履行基本法定义务。

二、主要内容

《办法》分成总则、网络安全事件分级、网络安全事件报告、法律责任、附则五章，共三十二条，主要内容如下:

第一章总则，明确目的和依据、适用范围、术语定义、向其他部门报告通报和社会监督机制。

第二章网络安全事件分级，明确网络安全事件分级管理要求，提出特别重大、重大、较大、一般等级网络安全事件的分级标准底线规则。

第三章网络安全事件报告，明确网络安全事件报告总体要求，细化报告流程、内容、时限、途径和责任认定处置等规定。

第四章法律责任，明确违规行为处理的相关规定，以及应当从轻减轻处罚的情形。

第五章附则，明确名词释义、解释权和适用性、生效期等内容。