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）

第一章 总则

第一条（目的和依据）为规范中国人民银行业务领域网络安全事件报告管理，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国中国人民银行法》等法律、行政法规，制定本办法。

第二条（适用范围）金融从业机构在中华人民共和国境内发生中国人民银行业务领域网络安全事件时，应当按照本办法规定向中国人民银行或者住所地中国人民银行分支机构报告，非中国人民银行业务领域网络安全事件无须按照本办法规定报告。法律、行政法规和中国人民银行对网络安全事件报告另有规定的，从其规定。

第三条（术语定义）本办法所称中国人民银行业务领域，是指依据法律、行政法规，党中央、国务院决定，由中国人民银行承担监督管理职责的业务领域。

本办法所称中国人民银行业务领域网络安全事件（以下简称网络安全事件），是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷和故障、不可抗力等因素，对金融从业机构建设、运营、维护的中国人民银行业务领域

网络或者处理的中国人民银行业务领域数据造成危害后果的事件。

本办法所称中国人民银行业务领域网络，是指用于支撑或者承载中国人民银行业务领域业务开展的不涉及国家秘密的网络。

本办法所称中国人民银行业务领域数据，是指中国人民银行业务领域内产生和收集的不涉及国家秘密的网络数据。

第四条（向其他部门报告与通报）国家有关部门和其他金融管理部门等对网络安全事件报告另有规定的，金融从业机构还应当从其规定报告。涉及危害计算机信息系统等违法犯罪的网络安全事件，金融从业机构还应当及时向公安机关报案。

中国人民银行加强与国家有关部门和其他金融管理部门间的网络安全事件报告共享，中国人民银行及其各级分支机构按照国家有关部门规定向其通报网络安全事件，并根据其他金融管理部门需要向其通报网络安全事件。

第五条（社会监督）任何个人和组织有权向中国人民银行或者住所地中国人民银行分支机构举报金融从业机构未按照本办法要求报告网络安全事件的行为，中国人民银行及其分支机构对举报人的相关信息予以保密。

第二章 网络安全事件分级

第六条（网络安全事件分级管理）金融从业机构应当在

本机构网络安全管理制度或者操作规程中明确网络安全事件分级标准（以下简称分级标准），将网络安全事件分为特别重大、重大、较大和一般四个等级。金融从业机构应当每年组织评估并视情更新分级标准。分级标准如有更新，应当报本机构网络安全直接责任人批准。

金融从业机构制定分级标准时，应当综合考虑网络安全事件对业务、资金、客户、舆情等的影响程度。针对与货币存取款、支付交易、税款缴库、银行间市场交易密切相关的中国人民银行业务领域网络制定分级标准时，金融从业机构应当差异化考虑网络安全事件在业务高峰时段和非业务高峰时段对业务处理的影响程度。

涉及中国人民银行业务领域数据泄露、篡改、破坏的，金融从业机构还应当结合中国人民银行业务领域数据安全管理相关规定，制定分级标准。

金融从业机构可针对网络安全等级保护第三级以上的中国人民银行业务领域网络，逐一细化制定专门适用的分级标准。

第七条（特别重大网络安全事件分级标准底线规则）符合下列情形之一的，应当分级为特别重大网络安全事件：

（一）与货币存取款、支付交易、税款缴库、银行间市场交易密切相关，属于金融基础设施或者服务客户规模达5000万人以上的中国人民银行业务领域网络，业务高峰时段两个以上省级行政区范围服务整体中断运行3小时以上或者单个省级行政区范围服务整体中断运行6小时以上的。

（二）服务客户的中国人民银行业务领域网络主要功能出现服务中断、超时报错等情形，影响客户的规模测算或者估算达1000万人以上的。

（三）涉及中国人民银行业务领域核心数据泄露、篡改、破坏的。

（四）泄露1000万条以上敏感个人信息或者1亿条以上个人信息的。

（五）网信部门、公安机关已明确应当分级为特别重大网络安全事件的。

（六）中国人民银行或其上海总部、省分行、自治区分行、直辖市分行、计划单列市分行研判并书面告知金融从业机构，应当分级为特别重大网络安全事件的。

第八条（重大网络安全事件分级标准底线规则）符合下列情形之一的，应当至少分级为重大网络安全事件:

（一）与货币存取款、支付交易、税款缴库、银行间市场交易密切相关，属于金融基础设施或者服务客户规模达5000万人以上的中国人民银行业务领域网络，业务高峰时段两个以上省级行政区范围服务整体中断运行1.5小时以上或者单个省级行政区范围服务整体中断运行3小时以上的。

（二）服务客户的中国人民银行业务领域网络主要功能出现服务中断、超时报错等情形，影响客户的规模测算或者估算达100万人以上的。

（三）涉及中国人民银行业务领域重要数据泄露、篡改、破坏的。

（四）泄露100万条以上敏感个人信息或者1000万条以上个人信息的。

（五）网信部门、公安机关已明确应当分级为重大网络安全事件的。

（六）中国人民银行或其上海总部、省分行、自治区分行、直辖市分行、计划单列市分行研判并书面告知金融从业机构，应当分级为重大网络安全事件的。

第九条（较大网络安全事件分级标准底线规则）符合下列情形之一的，应当至少分级为较大网络安全事件:

（一）与货币存取款、支付交易、税款缴库、银行间市场交易密切相关，属于金融基础设施或者服务客户规模达5000万人以上的中国人民银行业务领域网络，业务高峰时段两个以上省级行政区范围服务整体中断运行15分钟以上或者单个省级行政区范围服务整体中断运行30分钟以上的。

（二）服务客户的中国人民银行业务领域网络主要功能出现服务中断、超时报错等情形，影响客户的规模测算或者估算达10万人以上的。

（三）泄露500条以上敏感个人信息或者5万条以上个人信息的。

（四）网络安全事件引发舆情，出现相关舆情信息进入社交媒体、搜索引擎或者新闻网站热点榜等情形的。

（五）遭受勒索恶意程序攻击，已对中国人民银行业务领域网络或者中国人民银行业务领域数据构成实际威胁的。

（六）网信部门、公安机关已明确应当分级为较大网络

安全事件的。

第十条（一般网络安全事件分级标准底线规则）符合下列情形之一的，应当至少分级为一般网络安全事件:

（一）服务客户的中国人民银行业务领域网络，两个以上省级行政区范围服务整体中断运行 15 分钟以上或者单个省级行政区范围服务整体中断运行 30 分钟以上的。

（二）服务客户的中国人民银行业务领域网络主要功能出现服务中断、超时报错等情形，影响客户的规模测算或者估算达 1 万人以上的。

（三）非服务客户的中国人民银行业务领域网络主要功能出现服务中断、超时报错等情形，已持续 1 小时以上的。

（四）涉及中国人民银行业务领域数据泄露、篡改、破坏，导致一定社会危害的。

（五）泄露个人信息的。

（六）网信部门、公安机关已明确应当分级为一般网络安全事件的。

第十一条（涉及金融基础设施网络安全事件分级管理）与中国人民银行管理的金融基础设施业务交互功能异常相关的网络安全事件对应的分级标准，金融从业机构应当先征求金融基础设施运营机构意见并协商一致。

第十二条（事发事中分级）金融从业机构发生网络安全事件时，应当对照分级标准，综合确定网络安全事件等级。同时符合多个分级标准的，应当按照最高级别确定网络安全事件等级。对照分级标准无法准确确定网络安全事件等级

的，应当至少分级为较大网络安全事件。

因灾害或者信息基础设施故障，导致金融从业机构多个中国人民银行业务领域网络同时发生网络安全事件时，应当先分别确定网络安全事件等级，再按照各网络安全事件等级中的最高级别，确定整体的网络安全事件等级。

网络安全事件发展事态已达到更高级别分级标准的，金融从业机构应当立即调高网络安全事件等级。

第三章 网络安全事件报告

第十三条（报告总体要求）金融从业机构应当明确应急处置与报告的职责分工，确保网络安全事件报告及时、准确、完整，不得迟报、漏报或者瞒报。

金融从业机构应当健全网络安全风险监测预警体系，提升第一时间发现和报告网络安全事件的技术能力。

网络安全事件报告工作不应干扰或者影响业务恢复、存证溯源、客户解释、舆情应对等处置工作。

第十四条（报告流程）国家开发银行、政策性银行、国有商业银行、中国邮政储蓄银行、股份制银行总行发生网络安全事件时，应当向中国人民银行报告，其分支机构发生网络安全事件时，应当向住所地中国人民银行分支机构报告。中国人民银行所属单位及其管理的金融基础设施运营机构发生网络安全事件时，应当向中国人民银行报告。其他金融从业机构或其分支机构发生网络安全事件时，应当向住所地

中国人民银行分支机构报告；在保障报告时效性前提下，证券、期货、基金机构发生网络安全事件时，经中国证监会派出机构转通报同级中国人民银行分支机构。

中国人民银行地市分行和计划单列市分行接报辖区发生较大等级以上网络安全事件时，应当及时上报至中国人民银行省、自治区、直辖市分行。中国人民银行省、自治区、直辖市分行接报辖区发生重大等级以上网络安全事件时，应当及时上报至中国人民银行。

第十五条（事发报告）金融从业机构发生较大等级以上网络安全事件后，应于30分钟内报送网络安全事件事发简要报告，并在2小时内报送网络安全事件事发报告。

第十六条（事中报告）对于重大等级以上网络安全事件，金融从业机构应当至少每隔2小时进行事中进展报告，直至处置结束。处置过程中如出现调高网络安全事件等级、处置取得阶段性进展、发现新的问题等重要情况时，应当立即报告。

第十七条（事后调查总结报告）一般等级以上网络安全事件处置结束后，金融从业机构应当于10个工作日内报送事后调查总结报告。无法按时报送事后调查总结报告的，金融从业机构应当先按时报送初步报告，说明承诺报送报告的日期并按时报送。承诺日期原则上应在处置结束之日起40个工作日内。

第十八条（报告途径）金融从业机构网络安全事件的事发、事中报告，可通过电话、即时通信工具、邮件、传真或

者中国人民银行指定的信息报送系统报告。采用互联网邮件、传真方式报告的，应当通过电话或者即时通信工具确认中国人民银行或其分支机构已收悉。涉及敏感信息的，不应通过互联网渠道报告。

金融从业机构事后调查总结报告，应当加盖本机构或者承担报告职责内设部门公章，书面报送。中国人民银行对网络安全事件事后调查总结报告另有电子化报送要求的，金融从业机构还应当按照要求电子化报送。

第十九条（报告内容）网络安全事件事发简要报告的内容包括初次确定的网络安全事件等级、事发时间、依据网络安全事件分类分级指南国家标准确定的网络安全事件分类、影响的中国人民银行业务领域网络及其对应的网络安全保护等级、涉及的数据中心、报告机构和报告时间、报告人和联系方式。网络安全事件事发报告应当在简要报告内容基础上，增补影响范围和程度、已采取的措施和效果，网络攻击事件还应当增补分析研判情况。

网络安全事件事中报告应当在事发报告基础上，增补说明最新确定的网络安全事件等级、影响变化、处置进展和下一步拟采取的措施。如存在需中国人民银行或其分支机构协调支持处置的事项，应当一并说明。

网络安全事件事后调查总结报告应当包括最终确定的网络安全事件等级、处置历程回顾、影响、损失评估、技术或者管理根源分析、处置经验教训、后续改进措施、报告机构和报告时间、报告人和联系方式、签发人。

第二十条（涉及个人信息时的报告内容要求）金融从业机构发生网络安全事件涉及个人信息的，事后调查总结报告还应当说明本机构为有效避免网络安全事件危害所采取的补救措施、依法通知个人的情况和告知个人可以采取减轻危害措施的情况。

对于重大等级以上网络安全事件，前款所列内容应当在事中进展报告中提前予以说明。

第二十一条（涉及责任认定时的报告内容要求）较大等级以上网络安全事件的事后调查总结报告内容，还应当包括直接负责的主管人员和其他直接责任人员的责任认定和对应责任处理情况。

金融从业机构应当在本机构网络安全管理制度中综合考虑动机态度、客观条件、程序方法、后果影响、挽回损失等因素，明确不同责任处理的差异化适用情形。事后调查总结报告中对直接负责的主管人员和其他直接责任人员的处理措施，应当符合本机构网络安全管理制度要求。

第二十二条（涉及减免责任处理时的报告内容要求）满足下列条件之一并且能提供相关证明材料的，金融从业机构可根据直接负责的主管人员和其他直接责任人员具体承担职责，视情针对性减轻或者免除责任处理，但应当在事后调查总结报告中予以说明:

（一）已按本办法规定主动报告，同时按照预案有关程序立即进行处置，尽最大努力降低影响的。

（二）推广安全可信的网络产品和服务，过程中无明显

主观过错的。

（三）已切实落实中国人民银行网络安全、数据安全相关管理制度要求，并严格执行本机构网络安全、数据安全管理制度和操作规程相关职责要求的。

第二十三条（网络安全事件报告退回重新报送要求）中国人民银行或其分支机构认为金融从业机构网络安全事件事后调查总结报告存在内容缺失、原因分析不清、影响损失评估失实、责任认定或者处理不当等情形，退回事后调查总结报告并正式反馈修改意见的，金融从业机构应当在收到反馈之日起10个工作日内完善事后调查总结报告并重新报送。

第二十四条（风险通报的报告要求）金融从业机构收到中国人民银行或其分支机构通报的业务运行异常、疑似数据泄露、系统漏洞、安全缺陷等风险提示时，应当立即组织核查，采取必要处置措施。经核查风险属实已产生实际危害影响并构成网络安全事件的，金融从业机构应当按照本办法要求进行报告；风险不属实、未产生实际危害影响或者尚不构成网络安全事件的，应当根据通报要求按时反馈风险核查处置情况。

第二十五条（网络安全事件清单管理）金融从业机构应当建立网络安全事件台账，完整准确记录事发时间、事发报告时间、中国人民银行或其分支机构接报联系人和处置期间全部的网络安全事件报告内容。中国人民银行分支机构应当相应建立辖区网络安全事件台账。台账应当至少留存三年。

第四章 法律责任

第二十六条（网络安全事件配合调查）中国人民银行或其分支机构根据金融从业机构报告处置网络安全事件的情况，可以按照《中国人民银行执法检查程序规定》明确的程序，对金融从业机构依法实施现场检查，金融从业机构应当予以配合。

金融从业机构拒绝、阻碍中国人民银行或其分支机构实施现场检查的，依照《中华人民共和国网络安全法》第六十九条等相关法律、行政法规规定予以处罚。

第二十七条（违规行为的处罚）金融从业机构未按照本办法规定对网络安全事件进行分级、报告，或者制定的分级标准明显不合理，存在网络安全事件迟报、漏报、瞒报以及报告内容不准确、不完整并且被中国人民银行或其分支机构书面退回后重新报送仍不能满足本办法规定等情形的，中国人民银行及其分支机构依照《中华人民共和国网络安全法》第五十九条等相关法律、行政法规相关规定予以处罚；涉及中国人民银行业务领域数据泄露、篡改、破坏或者非法获取、非法利用的，依照《中华人民共和国数据安全法》第四十五条等相关法律、行政法规规定予以处罚；涉及个人信息泄露、篡改、丢失的，还可以依照《中华人民共和国个人信息保护法》第六十六条等相关法律、行政法规规定予以处罚。

金融从业机构收到中国人民银行或其分支机构通报的风险，如果风险确实存在，但未立即采取补救措施或者未按

照本办法规定按时反馈核查处置情况的，中国人民银行及其分支机构依照《中华人民共和国网络安全法》第六十条等相关法律、行政法规规定予以处罚；通报的风险为数据安全缺陷、漏洞并且确实存在，但金融从业机构未立即采取补救措施的，还可以依照《中华人民共和国数据安全法》第四十五条等相关法律、行政法规规定予以处罚。

第二十八条（从轻减轻处罚的情形）金融从业机构在接受中国人民银行或其分支机构检查时，主动供述检查人员尚未掌握的未按照本办法要求报告网络安全事件行为的，应当从轻或者减轻处罚。

第二十九条（违规行为的追责问责）中国人民银行分支机构未按照本办法规定报告网络安全事件，存在失职失责行为，造成重大损失、严重后果或者恶劣影响的，对直接负责的主管人员和其他直接责任人员依规依纪依法予以严肃追责问责。

第五章 附则

第三十条（名词释义）本办法下列用语的含义：

（一）金融从业机构，是指金融机构以及经中国人民银行批准设立或者认定的其他机构。

（二）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（三）网络安全直接责任人，是指本机构主管网络安全的领导班子成员。

（四）业务高峰时段，是指按年度统计分时平均业务量超过日平均业务量百分之三的时段，或者依据本机构制度列明的其他合理计算方式确定的时段。

（五）整体中断运行，是指因网络安全事件，某一时段内未处理和处理失败业务量与正常情况全部业务量的比例，经测算或者估算已经超过百分之七十。

（六）本办法所称“以上”均含本数。

第三十一条（解释权和适用性）本办法由中国人民银行负责解释。国家外汇领域网络安全事件报告由国家外汇管理局负责，具体制度可另行制定。

中国人民银行分支机构自身网络安全事件的报告管理，按照本办法对金融从业机构的规定执行。

第三十二条（生效期）本办法自2025年××月××日起施行。《银行计算机安全事件报告管理制度》（银发〔2002〕280号文印发）《中国人民银行计算机系统信息安全报告制度》（银发〔2010〕366号文印发）同时废止。