中华人民共和国工业信息化部 中央网络安全和信息化领导小组办公室、国家互联网信息办公室
互联网文件舆情声音汇编

（2015—2017）

互联网文件

2017年互联网相关文件

网络购买商品七日无理由退货暂行办法

（国家工商行政管理总局令第90号）

第一章 总 则

第一条 为保障《消费者权益保护法》七日无理由退货规定的实施，保护消费者合法权益，促进电子商务健康发展，根据《消费者权益保护法》等相关法律、行政法规，制定本办法。

第二条 消费者为生活消费需要通过网络购买商品，自收到商品之日起七日内依照《消费者权益保护法》第二十五条规定退货的，适用本办法。

第三条 网络商品销售者应当依法履行七日无理由退货义务。

网络交易平台提供者应当引导和督促平台上的网络商品销售者履行七日无理由退货义务，进行监督检查，并提供技术保障。

第四条 消费者行使七日无理由退货权利和网络商品销售者履行七日无理由退货义务都应当遵循公平、诚实信用的原则，遵守商业道德。

第五条 鼓励网络商品销售者作出比本办法更有利于消费者的无理由退货承诺。

第二章 不适用退货的商品范围和商品完好标准

第六条 下列商品不适用七日无理由退货规定：

（一）消费者定作的商品；

（二）鲜活易腐的商品；

（三）在线下载或者消费者拆封的音像制品、计算机软件等数字化商品；

（四）交付的报纸、期刊。

第七条 下列性质的商品经消费者在购买时确认，可以不适用七日无理由退货规定：

（一）拆封后易影响人身安全或者生命健康的商品，或者拆封后易导致商品品质发生改变的商品；

（二）一经激活或者试用后价值贬损较大的商品；

（三）销售时已明示的临近保质期的商品、有瑕疵的商品。

第八条 消费者退回的商品应当完好。

商品能够保持原有品质、功能，商品本身、配件、商标标识齐全的，视为商品完好。

消费者基于查验需要而打开商品包装，或者为确认商品的品质、功能而进行合理的调试不影响商品的完好。

第九条 对超出查验和确认商品品质、功能需要而使用商品，导致商品价值贬损较大的，视为商品不完好。具体判定标准如下：

（一）食品（含保健食品）、化妆品、医疗器械、计生用品：必要的一次性密封包装被损坏；

（二）电子电器类：进行未经授权的维修、改动，破坏、涂改强制性产品认证标志、指示标贴、机器序列号等，有难以恢复原状的外观类使用痕迹，或者产生激活、授权信息、不合理的个人使用数据留存等数据类使用痕迹；

（三）服装、鞋帽、箱包、玩具、家纺、家居类：商标标识被摘、标识被剪，商品受污、受损。

第三章 退货程序

第十条 选择无理由退货的消费者应当自收到商品之日起七日内向网络商品销售者发出退货通知。

七日期间自消费者签收商品的次日开始起算。

第十一条 网络商品销售者收到退货通知后应当及时向消费者提供真实、准确的退货地址、退货联系人、退货联系电话等有效联系信息。

消费者获得上述信息后应当及时退回商品，并保留退货凭证。

第十二条 消费者退货时应当将商品本身、配件及赠品一并退回。

赠品包括赠送的实物、积分、代金券、优惠券等形式。如果赠品不能一并退回，经营者可以要求消费者按照事先标明的赠品价格支付赠品价款。

第十三条 消费者退回的商品完好的，网络商品销售者应当在收到退回商品之日起七日内向消费者返还已支付的商品价款。

第十四条 退款方式比照购买商品的支付方式。经营者与消费者另有约定的，从其约定。

购买商品时采用多种方式支付价款的，一般应当按照各种支付方式的实际支付价款以相应方式退款。

除征得消费者明确表示同意的以外，网络商品销售者不应当自行指定其他退款方式。

第十五条 消费者采用积分、代金券、优惠券等形式支付价款的，网络商品销售者在消费者退还商品后应当以相应形式返还消费者。对积分、代金券、优惠券的使用和返还有约定的，可以从其约定。

第十六条 消费者购买商品时采用信用卡支付方式并支付手续费的，网络商品销售者退款时可以不退回手续费。

消费者购买商品时采用信用卡支付方式并被网络商品销售者免除手续费的，网络商品销售者可以在退款时扣除手续费。

第十七条 退货价款以消费者实际支出的价款为准。

套装或者满减优惠活动中的部分商品退货，导致不能再享受优惠的，根据购买时各商品价格进行结算，多退少补。

第十八条 商品退回所产生的运费依法由消费者承担。经营者与消费者另有约定的，按照约定。

消费者参加满足一定条件免运费活动，但退货后已不能达到免运费活动要求的，网络商品销售者在退款时可以扣除运费。

第十九条 网络商品销售者可以与消费者约定退货方式，但不应当限制消费者的退货方式。

网络商品销售者可以免费上门取货，也可以征得消费者同意后有偿上门取货。

第四章 特别规定

第二十条 网络商品销售者应当采取技术手段或者其他措施，对于本办法第六条规定的不适用七日无理由退货的商品进行明确标注。

符合本办法第七条规定的商品，网络商品销售者应当在商品销售必经流程中设置显著的确认程序，供消费者对单次购买行为进行确认。如无确认，网络商品销售者不得拒绝七日无理由退货。

第二十一条 网络交易平台提供者应当与其平台上的网络商品销售者订立协议，明确双方七日无理由退货各自的权利、义务和责任。

第二十二条 网络交易平台提供者应当依法建立、完善其平台七日无理由退货规则以及配套的消费者权益保护有关制度，在其平台上显著位置明示，并从技术上保证消费者能够便利、完整地阅览和保存。

第二十三条 网络交易平台提供者应当对其平台上的网络商品销售者履行七日无理由退货义务建立检查监控制度，发现有违反相关法律、法规、规章的，应当及时采取制止措施，并向网络交易平台提供者或者网络商品销售者所在地工商行政管理部门报告，必要时可以停止对其提供平台服务。

第二十四条 网络交易平台提供者应当建立消费纠纷和解和消费维权自律制度。消费者在网络交易平台上购买商品，因退货而发生消费纠纷或其合法权益受到损害时，要求网络交易平台提供者调解的，网络交易平台提供者应当调解；消费者通过其他渠道维权的，网络交易平台提供者应当向消费者提供其平台上的网络商品销售者的真实名称、地址和有效联系方式，积极协助消费者维护自身合法权益。

第二十五条 网络商品销售者应当建立完善的七日无理由退货商品检验和处理程序。

对能够完全恢复到初始销售状态的七日无理由退货商品，可以作为全新商品再次销售；对不能够完全恢复到初始销售状态的七日无理由退货商品而再次销售的，应当通过显著的方式将商品的实际情况明确标注。

第五章 监督检查

第二十六条 工商行政管理部门应当加强对网络商品销售者和网络交易平台提供者经营行为的监督检查，督促和引导其建立健全经营者首问和赔偿先付制度，依法履行网络购买商品七日无理由退货义务。

第二十七条 工商行政管理部门应当及时受理和依法处理消费者有关七日无理由退货的投诉、举报。

第二十八条 工商行政管理部门应当依照公正、公开、及时的原则，综合运用建议、约谈、示范等方式，加强对网络商品销售者和网络交易平台提供者履行七日无理由退货法定义务的行政指导。

第二十九条 工商行政管理部门在对网络商品交易的监督检查中，发现经营者存在拒不履行七日无理由退货义务，侵害消费者合法权益行为的，应当依法进行查处，同时将相关处罚信息计入信用档案，向社会公布。

第六章 法律责任

第三十条 网络商品销售者违反本办法第六条、第七条规定，擅自扩大不适用七日无理由退货的商品范围的，按照《消费者权益保护法》第五十六条第一款第（八）项规定予以处罚。

第三十一条 网络商品销售者违反本办法规定，有下列情形之一的，依照《消费者权益保护法》第五十六条第一款第（八）项规定予以处罚：

（一）未经消费者在购买时确认，擅自以商品不适用七日无理由退货为由拒绝退货，或者以消费者已拆封、查验影响商品完好为由拒绝退货的；

（二）自收到消费者退货要求之日起超过十五日未办理退货手续，或者未向消费者提供真实、准确的退货地址、退货联系人等有效联系信息，致使消费者无法办理退货手续的；

（三）在收到退回商品之日起超过十五日未向消费者返还已支付的商品价款的。

第三十二条 网络交易平台提供者违反本办法第二十二条规定，未在其平台显著位置明示七日无理由退货规则及配套的有关制度，或者未在技术上保证消费者能够便利、完整地阅览和保存的，予以警告，责令改正；拒不改正的，处以一万元以上三万元以下的罚款。

第三十三条 网络商品销售者违反本办法第二十五条规定，销售不能够完全恢复到初始状态的无理由退货商品，且未通过显著的方式明确标注商品实际情况的，违反其他法律、行政法规的，依照有关法律、行政法规的规定处罚；法律、行政法规未作规定的，予以警告，责令改正，并处一万元以上三万元以下的罚款。

第三十四条 网络交易平台提供者拒绝协助工商行政管理部门对涉嫌违法行为采取措施、开展调查的，予以警告，责令改正；拒不改正的，处三万元以下的罚款。

第七章 附 则

第三十五条 本办法所称工商行政管理部门，包括履行工商行政管理职能的市场监督管理部门。

第三十六条 网络商品销售者提供的商品不符合质量要求，消费者要求退货的，适用《消费者权益保护法》第二十四条以及其他相关规定。

第三十七条 经营者采用电视、电话、邮购等方式销售商品，依照本办法执行。

第三十八条 本办法由国家工商行政管理总局负责解释。

第三十九条 本办法自2017年3月15日起施行。

中央网信办关于印发《国家网络安全事件应急预案》的通知

中网办发文〔2017〕4号

各省、自治区、直辖市、新疆生产建设兵团党委网络安全和信息化领导小组，中央和国家机关各部委、各人民团体：

《国家网络安全事件应急预案》已经中央网络安全和信息化领导小组同意，现印发给你们，请认真组织实施。

中央网络安全和信息化领导小组办公室

2017年1月10日

国家网络安全事件应急预案

目 录

1 总则

1.1 编制目的

建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》和《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定。

1.3 适用范围

本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

1.4 事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1）符合下列情形之一的，为特别重大网络安全事件：

①重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

①重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

①重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

②国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

1.5 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

2 组织机构与职责

2.1 领导机构与职责

在中央网络安全和信息化领导小组（以下简称“领导小组”）的领导下，中央网络安全和信息化领导小组办公室（以下简称“中央网信办”）统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。

2.2 办事机构与职责

国家网络安全应急办公室（以下简称“应急办”）设在中央网信办，具体工作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的司局级同志为联络员，联络应急办工作。

2.3 各部门职责

中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

2.4 各省（区、市）职责

各省（区、市）网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

3 监测与预警

3.1 预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各省（区、市）、各部门将重要监测信息报应急办，应急办组织开展跨省（区、市）、跨部门的网络安全信息共享。

3.3 预警研判和发布

各省（区、市）、各部门组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省（区、市）、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警。

应急办组织研判，确定和发布红色预警和涉及多省（区、市）、多部门、多行业的预警。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

3.4 预警响应

3.4.1 红色预警响应

（1）应急办组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

（2）有关省（区、市）、部门网络安全事件应急指挥机构实行 24 小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报应急办。

（3）国家网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

（1）有关省（区、市）、部门网络安全事件应急指挥机构启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2）有关省（区、市）、部门及时将事态发展情况报应急办。应急办密切关注事态发展，有关重大事项及时通报相关省（区、市）和部门。

（3）国家网络安全应急技术支撑队伍保持联络畅通，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.3 黄色、蓝色预警响应

有关地区、部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

3.5 预警解除

预警发布部门或地区根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。

4.2 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I 级为最高响应级别。

4.2.1 Ⅰ级响应

属特别重大网络安全事件的，及时启动Ⅰ级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。应急办24小时值班。

有关省（区、市）、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责本省（区、市）、本部门应急处置工作或支援保障工作，24小时值班，并派员参加应急办工作。

有关省（区、市）、部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关省（区、市）和部门负责组织实施。

4.2.2 Ⅱ级响应

网络安全事件的Ⅱ级响应，由有关省（区、市）和部门根据事件的性质和情况确定。

（1）事件发生省（区、市）或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

（2）事件发生省（区、市）或部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报相关地区和部门。

（3）处置中需要其他有关省（区、市）、部门和国家网络安全应急技术支撑队伍配合和支持的，商应急办予以协调。相关省（区、市）、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

（4）有关省（区、市）和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 Ⅲ级、Ⅳ级响应

事件发生地区和部门按相关预案进行应急响应。

4.3 应急结束

4.3.1 Ⅰ级响应结束

应急办提出建议，报指挥部批准后，及时通报有关省（区、市）和部门。

4.3.2 Ⅱ级响应结束

由事件发生省（区、市）或部门决定，报应急办，应急办通报相关省（区、市）和部门。

5 调查与评估

特别重大网络安全事件由应急办组织有关部门和省（区、市）进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生地区或部门自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报应急办。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

6 预防工作

6.1 日常管理

各地区、各部门按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

6.2 演练

中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。

各省（区、市）、各部门每年至少组织一次预案演练，并将演练情况报中央网信办。

6.3 宣传

各地区、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

6.4 培训

各地区、各部门要将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

6.5 重要活动期间的预防措施

在国家重要活动、会议期间，各省（区、市）、各部门要加强网络安全事件的防范和应急响应，确保网络安全。应急办统筹协调网络安全保障工作，根据需要要求有关省（区、市）、部门启动红色预警响应。有关省（区、市）、部门加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 机构和人员

各地区、各部门、各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

7.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持网络安全企业提升应急处置能力，提供应急技术支援。中央网信办制定评估认定标准，组织评估和认定国家网络安全应急技术支撑队伍。各省（区、市）、各部门应配备必要的网络安全专业技术人才，并加强与国家网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。

7.3 专家队伍

建立国家网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各地区、各部门加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

7.5 基础平台

各地区、各部门加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

7.6 技术研发和产业促进

有关部门加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.7 国际合作

有关部门建立国际合作渠道，签订合作协定，必要时通过国际合作共同应对突发网络安全事件。

7.8 物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

7.9 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。

7.10 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

中央网信办及有关地区和部门对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励。

中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由中央网信办负责。

各省（区、市）、各部门、各单位要根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案。

8.2 预案解释

本预案由中央网信办负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

附件：

1. 网络安全事件分类
2. 名词术语
3. 网络和信息系统损失程度划分说明

附件 1

网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

附件 2

名词术语

一、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

（参考依据:《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)）

二、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果：

a）损害国防、国际关系；

b）损害国家财产、公共利益以及个人财产或人身安全；

c）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d）影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；

e）干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f）危害国家关键基础设施、政府信息系统安全；

g）影响市场秩序，造成不公平竞争，破坏市场规律；

h）可推论出国家秘密事项；

i）侵犯个人隐私、企业商业秘密和知识产权；

j）损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术云计算服务安全指南》（GB/T31167-2014））

附件 3

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a）特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b）严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c）较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d）较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

国家网信办启动互联网应用商店备案工作

为进一步促进互联网应用商店行业健康有序发展，规范移动互联网应用程序（APP）信息服务，依据《移动互联网应用程序信息服务管理规定》，国家互联网信息办公室日前下发《关于开展互联网应用商店备案工作的通知》，要求各省、自治区、直辖市互联网信息办公室于 1 月 16 日起，正式启动互联网应用商店备案工作。

国家网信办有关发言人表示，互联网应用商店作为 APP 的主要出入口，其分发渠道作用进一步凸显。与此同时，部分应用商店基本规范不健全、基础管理不到位，为谋取经济利益追求大而全的收录数量，对 APP 上架审核把关不严，导致一些传播违法违规信息、侵害用户合法权益、存在安全隐患的 APP 频现，社会反映强烈。

国家网信办有关发言人指出，开展互联网应用商店备案工作，是坚持依法治网、依法管网，落实《移动互联网应用程序信息服务管理规定》相关要求，夯实移动互联网管理工作基础、规范应用商店行业秩序的重要举措和关键环节。

国家网信办有关发言人介绍，互联网应用商店备案工作旨在督促应用商店落实主体责任，加强 APP 上架审核，促进移动互联网健康有序发展，将突出“三个申请”：一是应用商店业务运营需申请备案；二是应用商店备案事项变更需申请变更备案；三是应用商店停止服务需申请注销备案。

国家网信办有关发言人强调，通知要求互联网应用商店应按照 ICP 备案地或许可证申领地，向属地网信办现场提交纸质版与电子版备案材料，履行应用商店备案手续。各地网信办要严格审核备案信息，提供备案咨询服务，对拒不办理备案、提供虚假备案信息、违规经营情况严重的应用商店，要依法依规坚决查处。国家网信办将加强对备案工作监督检查，及时掌握应用商店基本情况和行业底数，适时组织提供统一查询服务，面向全社会公开备案应用商店信息。

工业和信息化部关于清理规范互联网网络接入服务市场的通知

工信部信管函[2017]32 号

各省、自治区、直辖市通信管理局，中国信息通信研究院，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司、中国广播电视网络有

限公司、中信网络有限公司，各互联网数据中心业务经营者、互联网接入服务业务经营者、内容分发网络业务经营者：

近年来，网络信息技术日新月异，云计算、大数据等应用蓬勃发展，我国互联网网络接入服务市场面临难得的发展机遇，但无序发展的苗头也随之显现，亟须整治规范。为进一步规范市场秩序，强化网络信息安全管理，促进互联网行业健康有序发展，工业和信息化部决定自即日起至2018年3月31日，在全国范围内对互联网网络接入服务市场开展清理规范工作。现将有关事项通知如下：

一、目标任务

依法查处互联网数据中心（IDC）业务、互联网接入服务（ISP）业务和内容分发网络（CDN）业务市场存在的无证经营、超范围经营、“层层转租”等违法行为，切实落实企业主体责任，加强经营许可和接入资源的管理，强化网络信息安全管理，维护公平有序的市场秩序，促进行业健康发展。

二、工作重点

（一）加强资质管理，查处非法经营

1.各通信管理局要对本辖区内提供IDC、ISP、CDN业务的企业情况进行摸底调查，杜绝以下非法经营行为：

（1）无证经营。即企业未取得相应的电信业务经营许可证，在当地擅自开展IDC、ISP、CDN等业务。

（2）超地域范围经营。即企业持有相应的电信业务经营许可证，业务覆盖地域不包括本地区，却在当地部署IDC机房及服务器，开展ISP接入服务等。

（3）超业务范围经营。即企业持有电信业务经营许可证，但超出许可的业务种类在当地开展IDC、ISP、CDN等业务。

（4）转租转让经营许可证。即持有相应的电信业务经营许可证的企业，以技术合作等名义向无证企业非法经营电信业务提供资质或资源等的违规行为。

2.在《电信业务分类目录（2015年版）》实施前已持有IDC许可证的企业，若实际已开展互联网资源协作服务业务或CDN业务，应在2017年3月31日之前，向原发证机关书面承诺在2017年年底前达到相关经营许可要求，并取得相应业务的电信经营许可证。

未按期承诺的，自2017年4月1日起，应严格按照其经营许可证规定的业务范围开展经营活动，不得经营未经许可的相关业务。未按承诺如期取得相应电信业务经营许可的，自2018年1月1日起，不得经营该业务。

（二）严格资源管理，杜绝违规使用

各基础电信企业、互联网网络接入服务企业对网络基础设施和 IP 地址、带宽等网络接入资源的使用情况进行全面自查，切实整改以下问题：

1.网络接入资源管理不到位问题。各基础电信企业应加强线路资源管理，严格审核租用方资质和用途，不得向无相应电信业务经营许可的企业和个人提供用于经营 IDC、ISP、CDN 等业务的网络基础设施和 IP 地址、带宽等网络接入资源。

2.违规自建或使用非法资源问题。IDC、ISP、CDN 企业不得私自建设通信传输设施，不得使用无相应电信业务经营许可资质的单位或个人提供的网络基础设施和 IP 地址、带宽等网络接入资源。

3.层层转租问题。IDC、ISP 企业不得将其获取的 IP 地址、带宽等网络接入资源转租给其他企业，用于经营 IDC、ISP 等业务。

4.违规开展跨境业务问题。未经电信主管部门批准，不得自行建立或租用专线（含虚拟专用网络 VPN）等其他信道开展跨境经营活动。基础电信企业向用户出租的国际专线，应集中建立用户档案，向用户明确使用用途仅供其内部办公专用，不得用于连接境内外的数据中心或业务平台开展电信业务经营活动。

（三）落实相关要求，夯实管理基础

贯彻落实《工业和信息化部关于进一步规范因特网数据中心（IDC）业务和因特网接入服务（ISP）业务市场准入工作的通告》（工信部电管函[2012]552 号，以下简称《通告》）关于资金、人员、场地、设施、技术方案和信息安全管理的要求，强化事前、事中、事后全流程管理。

1.2012 年 12 月 1 日前取得 IDC、ISP 许可证的企业，应参照《通告》关于资金、人员、场地、设施、技术方案和信息安全管理等方面的要求，建设相关系统，通过评测，并完成系统对接工作。

当前尚未达到相关要求的企业，应在 2017 年 3 月 31 日之前，向原发证机关书面承诺在 2017 年年底前达到相关要求，通过评测，并完成系统对接工作。未按期承诺或者未按承诺如期通过评测完成系统对接工作的，各通信管理局应当督促相应企业整改。

其中，各相关企业应按照《关于切实做好互联网信息安全管理系统建设与对接工作的通知》、《关于通报全国增值 IDC/ISP 企业互联网信息安全管理系统对接情况的函》和《互联网信息安全管理系统使用及运行管理办法（试行）》（工

信厅网安〔2016〕135号）要求，按期完成互联网信息安全管理系统建设、测评及系统对接工作。未按期完成的，企业2017年电信业务经营许可证年检不予通过。

2.新申请IDC（互联网资源协作服务）业务经营许可证的企业需建设ICP/IP地址/域名信息备案系统、企业接入资源管理平台、信息安全管理系统，落实IDC机房运行安全和网络信息安全要求，并通过相关评测。

3.新申请CDN业务经营许可证的企业需建设ICP/IP地址/域名信息备案系统、企业接入资源管理平台、信息安全管理系统，落实网络信息安全要求，并通过相关评测。

4.现有持证IDC企业申请扩大业务覆盖范围或在原业务覆盖范围新增机房、业务节点的，需要在新增范围内达到《通告》关于IDC机房运行安全和网络信息安全管理的要求，并通过相关评测。

5.现有持证ISP（含网站接入）企业申请扩大业务覆盖范围的，需要在新增业务覆盖地区内达到《通告》关于网络信息安全管理的要求，并通过相关评测。

6.现有持证CDN企业申请扩大业务覆盖范围或在原业务覆盖范围增加带宽、业务节点的，需要在新增范围内达到《通告》关于网络信息安全管理的要求，并通过相关评测。

三、保障措施

（一）政策宣贯引导，做好咨询服务

各通信管理局要利用各种方式做好政策宣贯和解读工作，公布电话受理相关举报和解答企业问题咨询，引导企业按照要求合法开展经营活动。中国信息通信研究院要做好相关评测支撑工作，协助部和各通信管理局做好政策宣贯、举报受理、企业问题解答等工作。

（二）全面开展自查，自觉清理整顿

各基础电信企业集团公司要组织下属企业全面自查，统一业务规程和相关要求，从合同约束、用途复查、违规问责等全流程加强规范管理，严防各类接入资源违规使用；对存在问题的要立即予以改正，并追究相关负责人责任。

各IDC、ISP、CDN企业要落实主体责任，按照本通知要求全面自查清理，及时纠正各类违规行为，确保经营资质合法合规，网络设施和线路资源使用规范，加强各项管理系统建设并通过评测。

（三）加强监督检查，严查违规行为

各通信管理局加强对企业落实情况的监督检查，发现违规问题要督促企业及时整改，对拒不整改的企业要依法严肃查处；情节严重的，应在年检工作中认定为年检不合格，将其行为依法列入企业不良信用记录，经营许可证到期时依法不予续期，并且基础电信企业在与其开展合作、提供接入服务时应当重点考虑其信用记录。部将结合信访举报、舆情反映等情况适时组织开展监督抽查。

（四）完善退出机制，做好善后工作

对未达到相关许可要求或被列入因存在违规行为被列入不良信用记录的企业，不得继续发展新用户。发证机关督促相关企业在此期间按照《电信业务经营许可管理办法》有关规定做好用户善后工作。向发证机关提交经营许可证注销申请的，发证机关应依法注销该企业的 IDC、ISP 经营许可证。

（五）完善信用管理，加强人员培训

积极发挥第三方机构优势，研究建立 IDC/ISP/CDN 企业信用评价机制，从基础设施、服务质量、网络和信息安全保障能力等多维度综合评定，引导企业重视自身信用状况、完善管理制度建设、规范市场经营行为。各通信管理局要加强对相关从业人员的技能培训，不断提高从业人员的业务素质和能力水平。

四、工作要求

（一）提高认识，加强组织领导

开展互联网网络接入服务市场规范清理工作是加强互联网行业管理和基础管理的重要内容，对夯实管理基础、促进行业健康有序发展具有重要意义。各相关单位要指定相关领导牵头负责，加强组织保障，抓好贯彻落实。

各通信管理局、基础电信企业集团公司、互联网网络接入服务企业要落实责任，按照本通知要求，制定工作方案，明确任务分工、工作进度和责任，细化工作、责任到人，确保本次规范清理工作各项任务按期完成。

（三）加强沟通，定期总结通报

各通信管理局、各基础电信企业集团公司要加强沟通协作，及时总结工作经验，每季度末向部（信息通信管理局）报送工作进展情况，发生重大问题随时报部。部（信息通信管理局）将建立情况通报制度，并定期向社会公示规范清理工作进展情况。

工业和信息化部

2017 年 1 月 17 日

工信部就《关于清理规范互联网网络接入服务市场的通知》答记者问

日前，工业和信息化部印发《关于清理规范互联网网络接入服务市场的通知》（以下简称《通知》）。就媒体感兴趣的问题，工业和信息化部信息通信管理局负责人作了回答。

问：《通知》出台的背景情况是什么？为何要出台这样一个政策？

答：近年来，我国云计算、大数据等应用蓬勃发展，以互联网数据中心业务（IDC）、互联网接入服务业务（ISP）和内容分发网络业务（CDN）为代表的互联网网络接入服务市场面临难得的发展机遇，但无证经营、无序发展的苗头也随之显现，层层转租、违规自建网络基础设施等带来的“黑带宽”、“下水道”等问题不容忽视，既破坏了正常的市场秩序，损害了广大用户的合法权益，也给国家网络和信息安全带来隐患。在此背景下，工业和信息化部出台了《关于清理规范互联网网络接入服务市场的通知》，在全国范围内开展清理规范工作，依法查处无证经营、超范围经营、“层层转租”等违法行为，切实落实企业主体责任，加强经营许可和接入资源的管理，强化网络信息安全管理，维护公平有序的市场秩序，促进行业健康发展。

问：《通知》开展的清理规范工作的重点是什么？

答：本次清理规范工作将在以下三方面开展重点工作：一是加强资质管理，重点查处无证经营和超范围经营等非法经营行为，督促企业合法持证开展经营活动；二是严格资源管理，重点打击“层层转租”等违规行为，清理网络接入服务市场存在的“黑带宽”、“下水道”；三是落实相关要求，夯实管理基础，推动接入服务企业加强技术手段建设，完成各项评测工作。

. . . . . .

预览完毕
想查看全文请购买图书！