网络安全法律资讯专辑

前言： 随着斯诺登“棱镜门”事件的曝光，我国不断加强网络安全保障，构建国家网络安全战略的重要性日益凸显，互联网法治建设明显提速，其中最为重要之一当属《网络安全法》。在立法调整对象上，该法聚焦我国网络安全面临的两大挑战，分别规范网络运行安全与网络信息安全，指向性、针对性都非常强；在立法基本原则上，该法既立足于维护网络空间主权和国家安全、社会公共利益，又坚持网络安全和信息化发展并重，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展；《网络安全法》及与之配套所涉及的法律实务对律师执业也提出更多的研究领域与执业机会。深圳律协信息网络委整理汇编目前网络安全法方面的法律法规及政策，为律师提升相关业务的法律合规性与执业技能水平提供参考。

2020 年 3 月 总第 4 期

深圳律师协会信息网络与电子商务法律专业委员会

目 录

汇编编辑：余祖舜律师　深圳律协信息网络委主任

排版校对：周世郁　　广东瀛尊律师事务所实习律师

中华人民共和国国家安全法

中华人民共和国主席令

第二十九号

《中华人民共和国国家安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第十五次会议于2015年7月1日通过，现予公布，自公布之日起施行。

中华人民共和国主席 习近平

2015年7月1日

目录

第一章 总则

第一条 为了维护国家安全，保卫人民民主专政的政权和中国特色社会主义制度，保护人民的根本利益，保障改革开放和社会主义现代化建设的顺利进行，实现中华民族伟大复兴，根据宪法，制定本法。

第二条 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。

第三条 国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。

第四条 坚持中国共产党对国家安全工作的领导，建立集中统一、高效权威的国家安全领导体制。

第五条 中央国家安全领导机构负责国家安全工作的决策和议事协调，研究制定、指导实施国家安全战略和有关重大方针政策，统筹协调国家安全重大事项和重要工作，推动国家安全法治建设。

第六条 国家制定并不断完善国家安全战略，全面评估国际、国内安全形势，明确国家安全战略的指导方针、中长期目标、重点领域的国家安全政策、工作任务和措施。

第七条 维护国家安全，应当遵守宪法和法律，坚持社会主义法治原则，尊重和保障人权，依法保护公民的权利和自由。

第八条 维护国家安全，应当与经济社会发展相协调。 国家安全工作应当统筹内部安全和外部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全。

第九条 维护国家安全，应当坚持预防为主、标本兼治，专门工作与群众路线相结合，充分发挥专门机关和其他有关机关维护国家安全的职能作用，广泛动员公民和组织，防范、制止和依法惩治危害国家安全的行为。

第十条 维护国家安全，应当坚持互信、互利、平等、协作，积极同外国政府和国际组织开展安全交流合作，履行国际安全义务，促进共同安全，维护世界和平。

第十一条 中华人民共和国公民、一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织，都有维护国家安全的责任和义务。 中国的主权和领土完整不容侵犯和分割。维护国家主权、统一和领土完整是包括港澳同胞和台湾同胞在内的全中国人民的共同义务。

第十二条 国家对在维护国家安全工作中作出突出贡献的个人和组织给予表彰和奖励。

第十三条 国家机关工作人员在国家安全工作和涉及国家安全活动中，滥用职权、玩忽职守、徇私舞弊的，依法追究法律责任。 任何个人和组织违反本法和有关法律，不履行维护国家安全义务或者从事危害国家安全活动的，依法追究法律责任。

第十四条 每年 4 月 15 日为全民国家安全教育日。

第二章 维护国家安全的任务

第十五条 国家坚持中国共产党的领导，维护中国特色社会主义制度，发展社会主义民主政治，健全社会主义法治，强化权力运行制约和监督机制，保障人民当家作主的各项权利。 国家防范、制止和依法惩治任何叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力的渗透、破坏、颠覆、分裂活动。

第十六条 国家维护和发展最广大人民的根本利益，保卫人民安全，创造良好生存发展条件和安定工作生活环境，保障公民的生命财产安全和其他合法权益。

第十七条 国家加强边防、海防和空防建设，采取一切必要的防卫和管控措施，保卫领陆、内水、领海和领空安全，维护国家领土主权和海洋权益。

第十八条 国家加强武装力量革命化、现代化、正规化建设，建设与保卫国家安全和发展利益需要相适应的武装力量；实施积极防御军事战略方针，防备和抵御侵略，制止武装颠覆和分裂；开展国际军事安全合作，实施联合国维和、国际救援、海上护航和维护国家海外利益的军事行动，维护国家主权、安全、领土完整、发展利益和世界和平。

第十九条 国家维护国家基本经济制度和社会主义市场经济秩序，健全预防和化解经济安全风险的制度机制，保障关系国民经济命脉的重要行业和关键领域、重点产业、重大基础设施和重大建设项目以及其他重大经济利益安全。

第二十条 国家健全金融宏观审慎管理和金融风险防范、处置机制，加强金融基础设施和基础能力建设，防范和化解系统性、区域性金融风险，防范和抵御外部金融风险的冲击。

第二十一条 国家合理利用和保护资源能源，有效管控战略资源能源的开发，加强战略资源能源储备，完善资源能源运输战略通道建设和安全保护措施，加强国际资源能源合作，全面提升应急保障能力，保障经济社会发展所需的资源能源持续、可靠和有效供给。

第二十二条 国家健全粮食安全保障体系，保护和提高粮食综合生产能力，完善粮食储备制度、流通体系和市场调控机制，健全粮食安全预警制度，保障粮食供给和质量安全。

第二十三条 国家坚持社会主义先进文化前进方向，继承和弘扬中华民族优秀传统文化，培育和践行社会主义核心价值观，防范和抵制不良文化的影响，掌握意识形态领域主导权，增强文化整体实力和竞争力。

第二十四条 国家加强自主创新能力建设，加快发展自主可控的战略高新技术和重要领域核心关键技术，加强知识产权的运用、保护和科技保密能力建设，保障重大技术和工程的安全。

第二十五条 国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

第二十六条 国家坚持和完善民族区域自治制度，巩固和发展平等团结互助和谐的社会主义民族关系。坚持各民族一律平等，加强民族交往、交流、交融，防范、制止和依法惩治民族分裂活动，维护国家统一、民族团结和社会和谐，实现各民族共同团结奋斗、共同繁荣发展。

第二十七条 国家依法保护公民宗教信仰自由和正常宗教活动，坚持宗教独立自主自办的原则，防范、制止和依法惩治利用宗教名义进行危害国家安全的违法犯罪活动，反对境外势力干涉境内宗教事务，维护正常宗教活动秩序。 国家依法取缔邪教组织，防范、制止和依法惩治邪教违法犯罪活动。

第二十八条 国家反对一切形式的恐怖主义和极端主义，加强防范和处置恐怖主义的能力建设，依法开展情报、调查、防范、处置以及资金监管等工作，依法取缔恐怖活动组织和严厉惩治暴力恐怖活动。

第二十九条 国家健全有效预防和化解社会矛盾的体制机制，健全公共安全体系，积极预防、减少和化解社会矛盾，妥善处置公共卫生、社会安全等影响国家安全和社会稳定的突发事件，促进社会和谐，维护公共安全和社会安定。

第三十条 国家完善生态环境保护制度体系，加大生态建设和环境保护力度，划定生态保护红线，强化生态风险的预警和防控，妥善处置突发环境事件，保障人民赖以生存发展的大气、水、土壤等自然环境和条件不受威胁和破坏，促进人与自然和谐发展。

第三十一条 国家坚持和平利用核能和核技术，加强国际合作，防止核扩散，完善防扩散机制，加强对核设施、核材料、核活动和核废料处置的安全管理、监管和保护，加强核事故应急体系和应急能力建设，防止、控制和消除核事故对公民生命健康和生态环境的危害，不断增强有效应对和防范核威胁、核攻击的能力。

第三十二条 国家坚持和平探索和利用外层空间、国际海底区域和极地，增强安全进出、科学考察、开发利用的能力，加强国际合作，维护我国在外层空间、国际海底区域和极地的活动、资产和其他利益的安全。

第三十三条 国家依法采取必要措施，保护海外中国公民、组织和机构的安全和正当权益，保护国家的海外利益不受威胁和侵害。

第三十四条 国家根据经济社会发展和国家发展利益的需要，不断完善维护国家安全的任务。

第三章 维护国家安全的职责

第三十五条 全国人民代表大会依照宪法规定，决定战争和和平的问题，行使宪法规定的涉及国家安全的其他职权。 全国人民代表大会常务委员会依照宪法规定，决定战争状态的宣布，决定全国总动员或者局部动员，决定全国或者个别省、自治区、直辖市进入紧急状态，行使宪法规定的和全国人民代表大会授予的涉及国家安全的其他职权。

第三十六条 中华人民共和国主席根据全国人民代表大会的决定和全国人民代表大会常务委员会的决定，宣布进入紧急状态，宣布战争状态，发布动员令，行使宪法规定的涉及国家安全的其他职权。

第三十七条 国务院根据宪法和法律，制定涉及国家安全的行政法规，规定有关行政措施，发布有关决定和命令；实施国家安全法律法规和政策；依照法律规定决定省、自治区、直辖市的范围内部分地区进入紧急状态；行使宪法法律规定的和全国人民代表大会及其常务委员会授予的涉及国家安全的其他职权。

第三十八条 中央军事委员会领导全国武装力量，决定军事战略和武装力量的作战方针，统一指挥维护国家安全的军事行动，制定涉及国家安全的军事法规，发布有关决定和命令。

第三十九条 中央国家机关各部门按照职责分工，贯彻执行国家安全方针政策和法律法规，管理指导本系统、本领域国家安全工作。

第四十条 地方各级人民代表大会和县级以上地方各级人民代表大会常务委员会在本行政区域内，保证国家安全法律法规的遵守和执行。 地方各级人民政府依照法律法规规定管理本行政区域内的国家安全工作。 香港特别行政区、澳门特别行政区应当履行维护国家安全的责任。

第四十一条 人民法院依照法律规定行使审判权，人民检察院依照法律规定行使检察权，惩治危害国家安全的犯罪。

第四十二条 国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。 有关军事机关在国家安全工作中依法行使相关职权。

第四十三条 国家机关及其工作人员在履行职责时，应当贯彻维护国家安全的原则。国家机关及其工作人员在国家安全工作和涉及国家安全活动中，应当严格依法履行职责，不得超越职权、滥用职权，不得侵犯个人和组织的合法权益。

第四章 国家安全制度

第一节 一般规定

第四十四条 中央国家安全领导机构实行统分结合、协调高效的国家安全制度与工作机制。

第四十五条 国家建立国家安全重点领域工作协调机制，统筹协调中央有关职能部门推进相关工作。

第四十六条 国家建立国家安全工作督促检查和责任追究机制，确保国家安全战略和重大部署贯彻落实。

第四十七条 各部门、各地区应当采取有效措施，贯彻实施国家安全战略。

第四十八条 国家根据维护国家安全工作需要，建立跨部门会商工作机制，就维护国家安全工作的重大事项进行会商研判，提出意见和建议。

第四十九条 国家建立中央与地方之间、部门之间、军地之间以及地区之间关于国家安全的协同联动机制。

第五十条 国家建立国家安全决策咨询机制，组织专家和有关方面开展对国家安全形势的分析研判，推进国家安全的科学决策。

第二节 情报信息

第五十一条 国家健全统一归口、反应灵敏、准确高效、运转顺畅的情报信息收集、研判和使用制度，建立情报信息工作协调机制，实现情报信息的及时收集、准确研判、有效使用和共享。

第五十二条 国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。 国家机关各部门在履行职责过程中，对于获取的涉及国家安全的有关信息应当及时上报。

第五十三条 开展情报信息工作，应当充分运用现代科学技术手段，加强对情报信息的鉴别、筛选、综合和研判分析。

第五十四条 情报信息的报送应当及时、准确、客观，不得迟报、漏报、瞒报和谎报。

第三节 风险预防、评估和预警

第五十五条 国家制定完善应对各领域国家安全风险预案。

第五十六条 国家建立国家安全风险评估机制，定期开展各领域国家安全风险调查评估。 有关部门应当定期向中央国家安全领导机构提交国家安全风险评估报告。

第五十七条 国家健全国家安全风险监测预警制度，根据国家安全风险程度，及时发布相应风险预警。

第五十八条 对可能即将发生或者已经发生的危害国家安全的事件，县级以上地方人民政府及其有关主管部门应当立即按照规定向上一级人民政府及其有关主管部门报告，必要时可以越级上报。

第四节 审查监管

第五十九条 国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

第六十条 中央国家机关各部门依照法律、行政法规行使国家安全审查职责，依法作出国家安全审查决定或者提出安全审查意见并监督执行。

第六十一条 省、自治区、直辖市依法负责本行政区域内有关国家安全审查和监管工作。

第五节 危机管控

第六十二条 国家建立统一领导、协同联动、有序高效的国家安全危机管控制度。

第六十三条 发生危及国家安全的重大事件，中央有关部门和有关地方根据中央国家安全领导机构的统一部署，依法启动应急预案，采取管控处置措施。

第六十四条 发生危及国家安全的特别重大事件，需要进入紧急状态、战争状态或者进行全国总动员、局部动员的，由全国人民代表大会、全国人民代表大会常务委员会或者国务院依照宪法和有关法律规定的权限和程序决定。

第六十五条 国家决定进入紧急状态、战争状态或者实施国防动员后，履行国家安全危机管控职责的有关机关依照法律规定或者全国人民代表大会常务委员会规定，有权采取限制公民和组织权利、增加公民和组织义务的特别措施。

第六十六条 履行国家安全危机管控职责的有关机关依法采取处置国家安全危机的管控措施，应当与国家安全危机可能造成的危害的性质、程度和范围相适应；有多种措施可供选择的，应当选择有利于最大程度保护公民、组织权益的措施。

第六十七条 国家健全国家安全危机的信息报告和发布机制。 国家安全危机事件发生后，履行国家安全危机管控职责的有关机关，应当按照规定准确、及时报告，并依法将有关国家安全危机事件发生、发展、管控处置及善后情况统一向社会发布。

第六十八条 国家安全威胁和危害得到控制或者消除后，应当及时解除管控处置措施，做好善后工作。

第五章 国家安全保障

第六十九条 国家健全国家安全保障体系，增强维护国家安全的能力。

第七十条 国家健全国家安全法律制度体系，推动国家安全法治建设。

第七十一条 国家加大对国家安全各项建设的投入，保障国家安全工作所需经费和装备。

第七十二条 承担国家安全战略物资储备任务的单位，应当按照国家有关规定和标准对国家安全物资进行收储、保管和维护，定期调整更换，保证储备物资的使用效能和安全。

第七十三条 鼓励国家安全领域科技创新，发挥科技在维护国家安全中的作用。

第七十四条 国家采取必要措施，招录、培养和管理国家安全工作专门人才和特殊人才。 根据维护国家安全工作的需要，国家依法保护有关机关专门从事国家安全工作人员的身份和合法权益，加大人身保护和安置保障力度。

第七十五条 国家安全机关、公安机关、有关军事机关开展国家安全专门工作，可以依法采取必要手段和方式，有关部门和地方应当在职责范围内提供支持和配合。

第七十六条 国家加强国家安全新闻宣传和舆论引导，通过多种形式开展国家安全宣传教育活动，将国家安全教育纳入国民教育体系和公务员教育培训体系，增强全民国家安全意识。

第六章 公民、组织的义务和权利

第七十七条 公民和组织应当履行下列维护国家安全的义务： （一）遵守宪法、法律法规关于国家安全的有关规定； （二）及时报告危害国家安全活动的线索； （三）如实提供所知悉的涉及危害国家安全活动的证据；（四）为国家安全工作提供便利条件或者其他协助；（五）向国家安全机关、公安机关和有关军事机关提供必要的支持和协助；（六）保守所知悉的国家秘密； （七）法律、行政法规规定的其他义务。 任何个人和组织不得有危害国家安全的行为，不得向危害国家安全的个人或者组织提供任何资助或者协助。

第七十八条 机关、人民团体、企业事业组织和其他社会组织应当对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止危害国家安全的行为。

第七十九条 企业事业组织根据国家安全工作的要求，应当配合有关部门采取相关安全措施。

第八十条 公民和组织支持、协助国家安全工作的行为受法律保护。 因支持、协助国家安全工作，本人或者其近亲属的人身安全面临危险的，可以向公安机关、国家安全机关请求予以保护。公安机关、国家安全机关应当会同有关部门依法采取保护措施。

第八十一条 公民和组织因支持、协助国家安全工作导致财产损失的，按照国家有关规定给予补偿；造成人身伤害或者死亡的，按照国家有关规定给予抚恤优待。

第八十二条 公民和组织对国家安全工作有向国家机关提出批评建议的权利，对国家机关及其工作人员在国家安全工作中的违法失职行为有提出申诉、控告和检举的权利。

第八十三条 在国家安全工作中，需要采取限制公民权利和自由的特别措施时，应当依法进行，并以维护国家安全的实际需要为限度。

第七章 附则

第八十四条 本法自公布之日起施行。

中华人民共和国网络安全法

主席令（第五十三号）

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过,现予公布,自2017年6月1日起施行。

中华人民共和国主席 习近平

2016年11月7日

目录

第一章 总 则

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主

义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营

者不得为其提供相关服务。国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服

务机构等之间的网络安全信息共享；（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章　网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不

得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章　监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。网络安全事

件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章　法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危

害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：（一）设置恶意程序的；（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网

络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；（二）拒绝、阻碍有关部门依法实施的监督检查的；（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附 则

第七十六条 本法下列用语的含义：（一）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。（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

全国人民代表大会常务委员会关于加强网络信息保护的决定

发布日期：2012-12-28 执行日期：2012-12-28

（第十一届全国人民代表大会常务委员会第三十次会议通过）

为了保护网络信息安全，保障公民、法人和其他组织的合法权益，维护国家安全和社会公共利益，特作如下决定：

一、国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。

任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。

二、网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。

网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。

三、网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

四、网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

五、网络服务提供者应当加强对其用户发布的信息的管理，发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

六、网络服务提供者为用户办理网站接入服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布服务，应当在与用户签订协议或者确认提供服务时，要求用户提供真实身份信息。

七、任何组织和个人未经电子信息接收者同意或者请求，或者电子信息接收者明确表示拒绝的，不得向其固定电话、移动电话或者个人电子邮箱发送商业性电子信息。

八、公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。

九、任何组织和个人对窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为,有权向有关主管部门举报、控告；接到举报、控告的部门应当依法及时处理。被侵权人可以依法提起诉讼。

十、有关主管部门应当在各自职权范围内依法履行职责，采取技术措施和其他必要措施，防范、制止和查处窃取或者以其他非法方式获取、出售或者非法向他人提供公民个人电子信息的违法犯罪行为以及其他网络信息违法犯罪行为。有关主管部门依法履行职责时，网络服务提供者应当予以配合，提供技术支持。

国家机关及其工作人员对在履行职责中知悉的公民个人电子信息应当予以保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

十一、对有违反本决定行为的，依法给予警告、罚款、没收违法所得、吊销许可证或者取消备案、关闭网站、禁止有关责任人员从事网络服务业务等处罚，记入社会信用档案并予以公布；构成违反治安管理行为的，依法给予治安管理处罚。构成犯罪的，依法追究刑事责任。侵害他人民事权益的，依法承担民事责任。

十二、本决定自公布之日起施行。

国家网络空间安全战略

2016 年 12 月 27 日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》，全文如下。

信息技术广泛应用和网络空间兴起发展，极大促进了经济社会繁荣进步，同时也带来了新的安全风险和挑战。网络空间安全（以下称网络安全）事关人类共同利益，事关世界和平与发展，事关各国国家安全。维护我国网络安全是协调推进全面建成小康社会、全面深化改革、全面依法治国、全面从严治党战略布局的重要举措，是实现“两个一百年”奋斗目标、实现中华民族伟大复兴中国梦的重要保障。为贯彻落实习近平主席关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益，制定本战略。

一、机遇和挑战

（一）重大机遇

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。

信息传播的新渠道。网络技术的发展，突破了时空限制，拓展了传播范围，创新了传播手段，引发了传播格局的根本性变革。网络已成为人们获取信息、学习交流的新渠道，成为人类知识传播的新载体。

生产生活的新空间。当今世界，网络深度融入人们的学习、生活、工作等方方面面，网络教育、创业、医疗、购物、金融等日益普及，越来越多的人通过网络交流思想、成就事业、实现梦想。

经济发展的新引擎。互联网日益成为创新驱动发展的先导力量，信息技术在国民经济各行业广泛应用，推动传统产业改造升级，催生了新技术、新业态、新产业、新模式，促进了经济结构调整和经济发展方式转变，为经济社会发展注入了新的动力。

文化繁荣的新载体。网络促进了文化交流和知识普及，释放了文化发展活力，推动了文化创新创造，丰富了人们精神文化生活，已经成为传播文化的新途径、提供公共文化服务的新手段。网络文化已成为文化建设的重要组成部分。

社会治理的新平台。网络在推进国家治理体系和治理能力现代化方面的作用日益凸显，电子政务应用走向深入，政府信息公开共享，推动了政府决策科学化、民主化、法治化，畅通了公民参与社会治理的渠道，成为保障公民知情权、参与权、表达权、监督权的重要途径。

交流合作的新纽带。信息化与全球化交织发展，促进了信息、资金、技术、人才等要素的全球流动，增进了不同文明交流融合。网络让世界变成了地球村，国际社会越来越成为你中有我、我中有你的命运共同体。

国家主权的新疆域。网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。尊重网络空间主权，维护网络安全，谋求共治，实现共赢，正在成为国际社会共识。

（二）严峻挑战

网络安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

网络渗透危害政治安全。政治稳定是国家发展、人民幸福的基本前提。利用网络干涉他国内政、攻击他国政治制度、煽动社会动乱、颠覆他国政权，以及大规模网络监控、网络窃密等活动严重危害国家政治安全和用户信息安全。

网络攻击威胁经济安全。网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。

网络有害信息侵蚀文化安全。网络上各种思想文化相互激荡、交锋，优秀传统文化和主流价值观面临冲击。网络谣言、颓废文化和淫秽、暴力、迷信等违背社会主义核心价值观的有害信息侵蚀青少年身心健康，败坏社会风气，误导价值取向，危害文化安全。网上道德失范、诚信缺失现象频发，网络文明程度亟待提高。

网络恐怖和违法犯罪破坏社会安全。恐怖主义、分裂主义、极端主义等势力利用网络煽动、策划、组织和实施暴力恐怖活动，直接威胁人民生命财产安全、社会秩序。计算机

病毒、木马等在网络空间传播蔓延，网络欺诈、黑客攻击、侵犯知识产权、滥用个人信息等不法行为大量存在，一些组织肆意窃取用户信息、交易数据、位置信息以及企业商业秘密，严重损害国家、企业和个人利益，影响社会和谐稳定。

网络空间的国际竞争方兴未艾。国际上争夺和控制网络空间战略资源、抢占规则制定权和战略制高点、谋求战略主动权的竞争日趋激烈。个别国家强化网络威慑战略，加剧网络空间军备竞赛，世界和平受到新的挑战。

网络空间机遇和挑战并存，机遇大于挑战。必须坚持积极利用、科学发展、依法管理、确保安全，坚决维护网络安全，最大限度利用网络空间发展潜力，更好惠及13亿多中国人民，造福全人类，坚定维护世界和平。

二、目标

以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

和平：信息技术滥用得到有效遏制，网络空间军备竞赛等威胁国际和平的活动得到有效控制，网络空间冲突得到有效防范。

安全：网络安全风险得到有效控制，国家网络安全保障体系健全完善，核心技术装备安全可控，网络和信息系统运行稳定可靠。网络安全人才满足需求，全社会的网络安全意识、基本防护技能和利用网络的信心大幅提升。

开放：信息技术标准、政策和市场开放、透明，产品流通和信息传播更加顺畅，数字鸿沟日益弥合。不分大小、强弱、贫富，世界各国特别是发展中国家都能分享发展机遇、共享发展成果、公平参与网络空间治理。

合作：世界各国在技术交流、打击网络恐怖和网络犯罪等领域的合作更加密切，多边、民主、透明的国际互联网治理体系健全完善，以合作共赢为核心的网络空间命运共同体逐步形成。

有序：公众在网络空间的知情权、参与权、表达权、监督权等合法权益得到充分保障，网络空间个人隐私获得有效保护，人权受到充分尊重。网络空间的国内和国际法律体系、标准规范逐步建立，网络空间实现依法有效治理，网络环境诚信、文明、健康，信息自由

流动与维护国家安全、公共利益实现有机统一。

三、原则

一个安全稳定繁荣的网络空间，对各国乃至世界都具有重大意义。中国愿与各国一道，加强沟通、扩大共识、深化合作，积极推进全球互联网治理体系变革，共同维护网络空间和平安全。

（一）尊重维护网络空间主权

网络空间主权不容侵犯，尊重各国自主选择发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利。各国主权范围内的网络事务由各国人民自己做主，各国有权根据本国国情，借鉴国际经验，制定有关网络空间的法律法规，依法采取必要措施，管理本国信息系统及本国疆域上的网络活动；保护本国信息系统和信息资源免受侵入、干扰、攻击和破坏，保障公民在网络空间的合法权益；防范、阻止和惩治危害国家安全和利益的有害信息在本国网络传播，维护网络空间秩序。任何国家都不搞网络霸权、不搞双重标准，不利用网络干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

（二）和平利用网络空间

和平利用网络空间符合人类的共同利益。各国应遵守《联合国宪章》关于不得使用或威胁使用武力的原则，防止信息技术被用于与维护国际安全与稳定相悖的目的，共同抵制网络空间军备竞赛、防范网络空间冲突。坚持相互尊重、平等相待，求同存异、包容互信，尊重彼此在网络空间的安全利益和重大关切，推动构建和谐网络世界。反对以国家安全为借口，利用技术优势控制他国网络和信息系统、收集和窃取他国数据，更不能以牺牲别国安全谋求自身所谓绝对安全。

（三）依法治理网络空间

全面推进网络空间法治化，坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。依法构建良好网络秩序，保护网络空间信息依法有序自由流动，保护个人隐私，保护知识产权。任何组织和个人在网络空间享有自由、行使权利的同时，须遵守法律，尊重他人权利，对自己在网络上的言行负责。

（四）统筹网络安全与发展

没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是一体之两翼、驱动之双轮。正确处理发展和安全的关系，坚持以安全保发展，以发展促安全。

安全是发展的前提，任何以牺牲安全为代价的发展都难以持续。发展是安全的基础，不发展是最大的不安全。没有信息化发展，网络安全也没有保障，已有的安全甚至会丧失。

四、战略任务

中国的网民数量和网络规模世界第一，维护好中国网络安全，不仅是自身需要，对于维护全球网络安全乃至世界和平都具有重大意义。中国致力于维护国家网络空间主权、安全、发展利益，推动互联网造福人类，推动网络空间和平利用和共同治理。

（一）坚定捍卫网络空间主权

根据宪法和法律法规管理我国主权范围内的网络活动，保护我国信息设施和信息资源安全，采取包括经济、行政、科技、法律、外交、军事等一切措施，坚定不移地维护我国网络空间主权。坚决反对通过网络颠覆我国国家政权、破坏我国国家主权的一切行为。

（二）坚决维护国家安全

防范、制止和依法惩治任何利用网络进行叛国、分裂国家、煽动叛乱、颠覆或者煽动颠覆人民民主专政政权的行为；防范、制止和依法惩治利用网络进行窃取、泄露国家秘密等危害国家安全的行为；防范、制止和依法惩治境外势力利用网络进行渗透、破坏、颠覆、分裂活动。

（三）保护关键信息基础设施

国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。

关键信息基础设施保护是政府、企业和全社会的共同责任，主管、运营单位和组织要按照法律法规、制度标准的要求，采取必要措施保障关键信息基础设施安全，逐步实现先评估后使用。加强关键信息基础设施风险评估。加强党政机关以及重点领域网站的安全防护，基层党政机关网站要按集约化模式建设运行和管理。建立政府、行业与企业的网络安

全信息有序共享机制，充分发挥企业在保护关键信息基础设施中的重要作用。

坚持对外开放，立足开放环境下维护网络安全。建立实施网络安全审查制度，加强供应链安全管理，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性，防止产品服务提供者和其他组织利用信息技术优势实施不正当竞争或损害用户利益。

（四）加强网络文化建设

加强网上思想文化阵地建设，大力培育和践行社会主义核心价值观，实施网络内容建设工程，发展积极向上的网络文化，传播正能量，凝聚强大精神力量，营造良好网络氛围。鼓励拓展新业务、创作新产品，打造体现时代精神的网络文化品牌，不断提高网络文化产业规模水平。实施中华优秀文化网上传播工程，积极推动优秀传统文化和当代文化精品的数字化、网络化制作和传播。发挥互联网传播平台优势，推动中外优秀文化交流互鉴，让各国人民了解中华优秀文化，让中国人民了解各国优秀文化，共同推动网络文化繁荣发展，丰富人们精神世界，促进人类文明进步。

加强网络伦理、网络文明建设，发挥道德教化引导作用，用人类文明优秀成果滋养网络空间、修复网络生态。建设文明诚信的网络环境，倡导文明办网、文明上网，形成安全、文明、有序的信息传播秩序。坚决打击谣言、淫秽、暴力、迷信、邪教等违法有害信息在网络空间传播蔓延。提高青少年网络文明素养，加强对未成年人上网保护，通过政府、社会组织、社区、学校、家庭等方面的共同努力，为青少年健康成长创造良好的网络环境。

（五）打击网络恐怖和违法犯罪

加强网络反恐、反间谍、反窃密能力建设，严厉打击网络恐怖和网络间谍活动。

坚持综合治理、源头控制、依法防范，严厉打击网络诈骗、网络盗窃、贩枪贩毒、侵害公民个人信息、传播淫秽色情、黑客攻击、侵犯知识产权等违法犯罪行为。

（六）完善网络治理体系

坚持依法、公开、透明管网治网，切实做到有法可依、有法必依、执法必严、违法必究。健全网络安全法律法规体系，制定出台网络安全法、未成年人网络保护条例等法律法规，明确社会各方面的责任和义务，明确网络安全管理要求。加快对现行法律的修订和解释，使之适用于网络空间。完善网络安全相关制度，建立网络信任体系，提高网络安全管理的科学化规范化水平。

加快构建法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的网络治理体系，推进网络社会组织管理创新，健全基础管理、内容管理、行业管理以及网络违法犯罪防范和打击等工作联动机制。加强网络空间通信秘密、言论自由、商业秘密，以及名誉权、财产权等合法权益的保护。

鼓励社会组织等参与网络治理，发展网络公益事业，加强新型网络社会组织建设。鼓励网民举报网络违法行为和不良信息。

（七）夯实网络安全基础

坚持创新驱动发展，积极创造有利于技术创新的政策环境，统筹资源和力量，以企业为主体，产学研用相结合，协同攻关、以点带面、整体推进，尽快在核心技术上取得突破。重视软件安全，加快安全可信产品推广应用。发展网络基础设施，丰富网络空间信息内容。实施“互联网+”行动，大力发展网络经济。实施国家大数据战略，建立大数据安全管理制度，支持大数据、云计算等新一代信息技术创新和应用。优化市场环境，鼓励网络安全企业做大做强，为保障国家网络安全夯实产业基础。

建立完善国家网络安全技术支撑体系。加强网络安全基础理论和重大问题研究。加强网络安全标准化和认证认可工作，更多地利用标准规范网络空间行为。做好等级保护、风险评估、漏洞发现等基础性工作，完善网络安全监测预警和网络安全重大事件应急处置机制。

实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境。办好网络安全宣传周活动，大力开展全民网络安全宣传教育。推动网络安全教育进教材、进学校、进课堂，提高网络媒介素养，增强全社会网络安全意识和防护技能，提高广大网民对网络违法有害信息、网络欺诈等违法犯罪活动的辨识和抵御能力。

（八）提升网络空间防护能力

网络空间是国家主权的新疆域。建设与我国国际地位相称、与网络强国相适应的网络空间防护力量，大力发展网络安全防御手段，及时发现和抵御网络入侵，铸造维护国家网络安全的坚强后盾。

（九）强化网络空间国际合作

在相互尊重、相互信任的基础上，加强国际网络空间对话合作，推动互联网全球治理

体系变革。深化同各国的双边、多边网络安全对话交流和信息沟通，有效管控分歧，积极参与全球和区域组织网络安全合作，推动互联网地址、根域名服务器等基础资源管理国际化。

支持联合国发挥主导作用，推动制定各方普遍接受的网络空间国际规则、网络空间国际反恐公约，健全打击网络犯罪司法协助机制，深化在政策法律、技术创新、标准规范、应急响应、关键信息基础设施保护等领域的国际合作。

加强对发展中国家和落后地区互联网技术普及和基础设施建设的支持援助，努力弥合数字鸿沟。推动“一带一路”建设，提高国际通信互联互通水平，畅通信息丝绸之路。搭建世界互联网大会等全球互联网共享共治平台，共同推动互联网健康发展。通过积极有效的国际合作，建立多边、民主、透明的国际互联网治理体系，共同构建和平、安全、开放、合作、有序的网络空间。

网络空间国际合作战略

2017 年 3 月 1 日，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室今天共同发布《网络空间国际合作战略》。

目录

序言

“网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体。”

——中国国家主席习近平，2015 年 12 月 16 日

当今世界，以互联网为代表的信息技术日新月异，引领了社会生产新变革，创造了人类生活新空间，拓展了国家治理新领域，极大提高了人类认识世界、改造世界的能力。

作为人类社会的共同财富，互联网让世界变成了“地球村”。各国在网络空间互联互通，利益交融，休戚与共。维护网络空间和平与安全，促进开放与合作，共同构建网络空间命运共同体，符合国际社会的共同利益，也是国际社会的共同责任。

《网络空间国际合作战略》全面宣示中国在网络空间相关国际问题上的政策立场，系统阐释中国开展网络领域对外工作的基本原则、战略目标和行动要点，旨在指导中国今后一个时期参与网络空间国际交流与合作，推动国际社会携手努力，加强对话合作，共同构建和平、安全、开放、合作、有序的网络空间，建立多边、民主、透明的全球互联网治理体系。

第一章 机遇与挑战

在世界多极化、经济全球化、文化多样化深入发展，全球治理体系深刻变革的背景下，人类迎来了信息革命的新时代。以互联网为代表的信息通信技术日新月异，深刻改变了人们的生产和生活方式，日益激励市场创新、促进经济繁荣、推动社会发展。网络空间越来越成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。

网络空间给人类带来巨大机遇，同时也带来了不少新的课题和挑战，网络空间的安全与稳定成为攸关各国主权、安全和发展利益的全球关切。互联网领域发展不平衡、规则不健全、秩序不合理等问题日益凸显。国家和地区间的“数字鸿沟”不断拉大。关键信息基础设施存在较大风险隐患。全球互联网基础资源管理体系难以反映大多数国家意愿和利益。网络恐怖主义成为全球公害，网络犯罪呈蔓延之势。滥用信息通信技术干涉别国内政、从

事大规模网络监控等活动时有发生。网络空间缺乏普遍有效规范各方行为的国际规则，自身发展受到制约。

面对问题和挑战，任何国家都难以独善其身，国际社会应本着相互尊重、互谅互让的精神，开展对话与合作，以规则为基础实现网络空间全球治理。

第二章 基本原则

中国始终是世界和平的建设者、全球发展的贡献者、国际秩序的维护者。中国坚定不移走和平发展道路，坚持正确义利观，推动建立合作共赢的新型国际关系。中国网络空间国际合作战略以和平发展为主题，以合作共赢为核心，倡导和平、主权、共治、普惠作为网络空间国际交流与合作的基本原则。

一、和平原则

网络空间互联互通，各国利益交融不断深化，一个安全稳定繁荣的网络空间，对各国乃至世界都具有重大意义。

国际社会要切实遵守《联合国宪章》宗旨与原则，特别是不使用或威胁使用武力、和平解决争端的原则，确保网络空间的和平与安全。各国应共同反对利用信息通信技术实施敌对行动和侵略行径，防止网络军备竞赛，防范网络空间冲突，坚持以和平方式解决网络空间的争端。应摒弃冷战思维、零和博弈和双重标准，在充分尊重别国安全的基础上，以合作谋和平，致力于在共同安全中实现自身安全。

网络恐怖主义是影响国际和平与安全的新威胁。国际社会要采取切实措施，预防并合作打击网络恐怖主义活动。防范恐怖分子利用网络宣传恐怖极端思想，策划和实施恐怖主义活动。

二、主权原则

《联合国宪章》确立的主权平等原则是当代国际关系的基本准则，覆盖国与国交往各个领域，也应该适用于网络空间。国家间应该相互尊重自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利，不搞网络霸权，不干涉他国内政，不从事、纵容或支持危害他国国家安全的网络活动。

明确网络空间的主权，既能体现各国政府依法管理网络空间的责任和权利，也有助于推动各国构建政府、企业和社会团体之间良性互动的平台，为信息技术的发展以及国际交流与合作营造一个健康的生态环境。

各国政府有权依法管网，对本国境内信息通信基础设施和资源、信息通信活动拥有管辖权，有权保护本国信息系统和信息资源免受威胁、干扰、攻击和破坏，保障公民在网络空间的合法权益。各国政府有权制定本国互联网公共政策和法律法规，不受任何外来干预。各国在根据主权平等原则行使自身权利的同时，也需履行相应的义务。各国不得利用信息通信技术干涉别国内政，不得利用自身优势损害别国信息通信技术产品和服务供应链安全。

三、共治原则

网络空间是人类共同的活动空间，需要世界各国共同建设，共同治理。网络空间国际治理，首先应坚持多边参与。国家不分大小、强弱、贫富，都是国际社会平等成员，都有权通过国际网络治理机制和平台，平等参与网络空间的国际秩序与规则建设，确保网络空间的未来发展由各国人民共同掌握。

其次，应坚持多方参与。应发挥政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各主体作用，构建全方位、多层面的治理平台。各国应加强沟通交流，完善网络空间对话协商机制，共同制定网络空间国际规则。联合国作为重要渠道，应充分发挥统筹作用，协调各方立场，凝聚国际共识。其它国际机制和平台也应发挥各自优势，提供有益补充。国际社会应共同管理和公平分配互联网基础资源，建立多边、民主、透明的全球互联网治理体系，实现互联网资源共享、责任共担、合作共治。

四、普惠原则

互联网与各行业的融合发展，对各国经济结构、社会形态和创新体系产生着全局性、革命性影响，为世界经济增长和实现可持续发展目标提供了强劲动力。促进互联网效益普遍惠及各地区和国家，将为 2030 年可持续发展议程的有效落实提供助力。

国际社会应不断推进互联网领域开放合作，丰富开放内涵，提高开放水平，搭建更多沟通合作平台，推动在网络空间优势互补、共同发展，确保人人共享互联网发展成果，实现信息社会世界峰会确定的建设以人为本、面向发展、包容性的信息社会目标。

各国应积极推动双边、区域和国际发展合作，特别是应加大对发展中国家在网络能力建设上的资金和技术援助，帮助他们抓住数字机遇，跨越“数字鸿沟”。

第三章 战略目标

中国参与网络空间国际合作的战略目标是：坚定维护中国网络主权、安全和发展利益，保障互联网信息安全有序流动，提升国际互联互通水平，维护网络空间和平安全稳定，推

动网络空间国际法治，促进全球数字经济发展，深化网络文化交流互鉴，让互联网发展成果惠及全球，更好造福各国人民。

一、维护主权与安全

中国致力于维护网络空间和平安全，以及在国家主权基础上构建公正合理的网络空间国际秩序，并积极推动和巩固在此方面的国际共识。中国坚决反对任何国家借网络干涉别国内政，主张各国有权利和责任维护本国网络安全，通过国家法律和政策保障各方在网络空间的正当合法权益。 网络空间加强军备、强化威慑的倾向不利于国际安全与战略互信。中国致力于推动各方切实遵守和平解决争端、不使用或威胁使用武力等国际关系基本准则，建立磋商与调停机制，预防和避免冲突，防止网络空间成为新的战场。

网络空间国防力量建设是中国国防和军队现代化建设的重要内容，遵循一贯的积极防御军事战略方针。中国将发挥军队在维护国家网络空间主权、安全和发展利益中的重要作用，加快网络空间力量建设，提高网络空间态势感知、网络防御、支援国家网络空间行动和参与国际合作的能力，遏控网络空间重大危机，保障国家网络安全，维护国家安全和社会稳定。

二、构建国际规则体系

网络空间作为新疆域，亟需制定相关规则和行为规范。中国主张在联合国框架下制定各国普遍接受的网络空间国际规则和国家行为规范，确立国家及各行为体在网络空间应遵循的基本准则，规范各方行为，促进各国合作，以维护网络空间的安全、稳定与繁荣。中国支持并积极参与国际规则制定进程，并将继续与国际社会加强对话合作，作出自己的贡献。

中国是网络安全的坚定维护者。中国也是黑客攻击的受害国。中国反对任何形式的黑客攻击，不论何种黑客攻击，都是违法犯罪行为，都应该根据法律和相关国际公约予以打击。网络攻击通常具有跨国性、溯源难等特点，中国主张各国通过建设性协商合作，共同维护网络空间安全。

三、促进互联网公平治理

中国主张通过国际社会平等参与和共同决策，构建多边、民主、透明的全球互联网治理体系。各国应享有平等参与互联网治理的权利。应公平分配互联网基础资源，共同管理

互联网根服务器等关键信息基础设施。要确保相关国际进程的包容与开放，加强发展中国家的代表性和发言权。

中国支持加强包括各国政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各利益攸关方的沟通与合作。各利益攸关方应在上述治理模式中发挥与自身角色相匹配的作用，政府应在互联网治理特别是公共政策和安全中发挥关键主导作用，实现共同参与、科学管理、民主决策。

四、保护公民合法权益

中国支持互联网的自由与开放，充分尊重公民在网络空间的权利和基本自由，保障公众在网络空间的知情权、参与权、表达权、监督权，保护网络空间个人隐私。同时，网络空间不是“法外之地”，网络空间与现实社会一样，既要提倡自由，也要保持秩序。中国致力于推动网络空间有效治理，实现信息自由流动与国家安全、公共利益有机统一。

五、促进数字经济合作

中国大力实施网络强国战略、国家信息化战略、国家大数据战略、“互联网+”行动计划，大力发展电子商务，着力推动互联网和实体经济深度融合发展，促进资源配置优化，促进全要素生产率提升，为推动创新发展、转变经济增长方式、调整经济结构发挥积极作用。

中国秉持公平、开放、竞争的市场理念，在自身发展的同时，坚持合作和普惠原则，促进世界范围内投资和贸易发展，推动全球数字经济发展。中国主张推动国际社会公平、自由贸易，反对贸易壁垒和贸易保护主义，促进建立开放、安全的数字经济环境，确保互联网为经济发展和创新服务。中国主张进一步推动实现公平合理普遍的互联网接入、互联网技术的普及化、互联网语言的多样性，加强中国同其他国家和地区在网络安全和信息技术方面的交流与合作，共同推进互联网技术的发展和创新，确保所有人都能平等分享数字红利，实现网络空间的可持续发展。

中国坚持以安全保发展，以发展促安全。要保持数字经济健康、强劲发展，既不能追求绝对安全阻碍发展的活力、限制开放互通、禁锢技术创新，也不能以市场自由化、贸易自由化为由，回避必要的安全监管措施。各国、各地区互联网发展水平和网络安全防护能力不同，应为广大发展中国家提升网络安全能力提供力所能及的援助，弥合发展中国家和发达国家间的“数字鸿沟”，实现数字经济互利共赢，补齐全球网络安全短板。

六、打造网上文化交流平台

互联网是传播人类优秀文化、弘扬正能量的重要载体。网络空间是人类共同的精神家园。各国应加强合作，共同肩负起运用互联网传承优秀文化的重任，培育和发展积极向上的网络文化，发挥文化滋养人类、涵养社会、促进经济发展的重要作用，共同推动网络文明建设和网络文化繁荣发展。

中国愿同各国一道，发挥互联网传播平台优势，通过互联网架设国际交流桥梁，促进各国优秀文化交流互鉴。加强网络文化传播能力建设，推动国际网络文化的多样性发展，丰富人们精神世界，促进人类文明进步。

第四章 行动计划

中国将积极参与网络领域相关国际进程，加强双边、地区及国际对话与合作，增进国际互信，谋求共同发展，携手应对威胁，以期最终达成各方普遍接受的网络空间国际规则，构建公正合理的全球网络空间治理体系。

一、倡导和促进网络空间和平与稳定

参与双多边建立信任措施的讨论，采取预防性外交举措，通过对话和协商的方式应对各种网络安全威胁。

加强对话，研究影响国际和平与安全的网络领域新威胁，共同遏制信息技术滥用，防止网络空间军备竞赛。

推动国际社会就网络空间和平属性展开讨论，从维护国际安全和战略互信、预防网络冲突角度，研究国际法适用网络空间问题。

二、推动构建以规则为基础的网络空间秩序

发挥联合国在网络空间国际规则制定中的重要作用，支持并推动联合国大会通过信息和网络安全相关决议，积极推动并参与联合国信息安全问题政府专家组等进程。

上海合作组织成员国于 2015 年 1 月向联大提交了“信息安全国际行为准则”更新案文。“准则”是国际上第一份全面系统阐述网络空间行为规范的文件，是中国等上合组织成员国为推动国际社会制定网络空间行为准则提供的重要公共安全产品。中国将继续就该倡议加强国际对话，争取对该倡议广泛的国际理解与支持。

支持国际社会在平等基础上普遍参与有关网络问题的国际讨论和磋商。

三、不断拓展网络空间伙伴关系

中国致力于与国际社会各方建立广泛的合作伙伴关系，积极拓展与其他国家的网络事务对话机制，广泛开展双边网络外交政策交流和务实合作。

举办世界互联网大会（乌镇峰会）等国际会议，与有关国家继续举行双边互联网论坛，在中日韩、东盟地区论坛、博鳌亚洲论坛等框架下举办网络议题研讨活动等，拓展网络对话合作平台。

推动深化上合组织、金砖国家网络安全务实合作。促进东盟地区论坛网络安全进程平衡发展。积极推动和支持亚信会议、中非合作论坛、中阿合作论坛、中拉论坛、亚非法律协商组织等区域组织开展网络安全合作。推进亚太经合组织、二十国集团等组织在互联网和数字经济等领域合作的倡议。探讨与其他地区组织在网络领域的交流对话。

四、积极推进全球互联网治理体系改革

参与联合国信息社会世界峰会成果落实后续进程，推动国际社会巩固和落实峰会成果共识，公平分享信息社会发展成果，并将加强信息社会建设和互联网治理列为审议的重要议题。

推进联合国互联网治理论坛机制改革，促进论坛在互联网治理中发挥更大作用。加强论坛在互联网治理事务上的决策能力，推动论坛获得稳定的经费来源，在遴选相关成员、提交报告等方面制定公开透明的程序。

参加旨在促进互联网关键资源公平分配和管理的国际讨论，积极推动互联网名称和数字地址分配机构国际化改革，使其成为具有真正独立性的国际机构，不断提高其代表性和决策、运行的公开透明。积极参与和推动世界经济论坛“互联网的未来”行动倡议等全球互联网治理平台活动。

五、深化打击网络恐怖主义和网络犯罪国际合作

探讨国际社会合作打击网络恐怖主义的行为规范及具体措施，包括探讨制定网络空间国际反恐公约，增进国际社会在打击网络犯罪和网络恐怖主义问题上的共识，并为各国开展具体执法合作提供依据。

支持并推动联合国安理会在打击网络恐怖主义国际合作问题上发挥重要作用。

支持并推动联合国开展打击网络犯罪的工作,参与联合国预防犯罪和刑事司法委员会、联合国网络犯罪问题政府专家组等机制的工作，推动在联合国框架下讨论、制定打击网络犯罪的全球性国际法律文书。

加强地区合作，依托亚太地区年度会晤协作机制开展打击信息技术犯罪合作，积极参加东盟地区论坛等区域组织相关合作，推进金砖国家打击网络犯罪和网络恐怖主义的机制安排。

加强与各国打击网络犯罪和网络恐怖主义的政策交流与执法等务实合作。积极探索建立打击网络恐怖主义机制化对话交流平台，与其他国家警方建立双边警务合作机制，健全打击网络犯罪司法协助机制，加强打击网络犯罪技术经验交流。

六、倡导对隐私权等公民权益的保护

支持联合国大会及人权理事会有关隐私权保护问题的讨论，推动网络空间确立个人隐私保护原则。推动各国采取措施制止利用网络侵害个人隐私的行为，并就尊重和保护网络空间个人隐私的实践和做法进行交流。

促进企业提高数据安全保护意识，支持企业加强行业自律，就网络空间个人信息保护最佳实践展开讨论。推动政府和企业加强合作，共同保护网络空间个人隐私。

七、推动数字经济发展和数字红利普惠共享

推动落实联合国信息社会世界峰会确定的建设以人为本、面向发展、包容性的信息社会目标，以此推进落实 2030 年可持续发展议程。

支持基于互联网的创新创业，促进工业、农业、服务业数字化转型。促进中小微企业信息化发展。促进信息通信技术领域投资。扩大宽带接入，提高宽带质量。提高公众的数字技能，提高数字包容性。增强在线交易的可用性、完整性、保密性和可靠性，发展可信、稳定和可靠的互联网应用。

支持向广大发展中国家提供网络安全能力建设援助，包括技术转让、关键信息基础设施建设和人员培训等，将“数字鸿沟”转化为数字机遇，让更多发展中国家和人民共享互联网带来的发展机遇。

推动制定完善的网络空间贸易规则，促进各国相关政策的有效协调。开展电子商务国际合作，提高通关、物流等便利化水平。保护知识产权，反对贸易保护主义，形成世界网络大市场，促进全球网络经济的繁荣发展。

加强互联网技术合作共享，推动各国在网络通信、移动互联网、云计算、物联网、大数据等领域的技术合作，共同解决互联网技术发展难题，共促新产业、新业态的发展。加强人才交流，联合培养创新型网络人才。

紧密结合“一带一路”建设，推动并支持中国的互联网企业联合制造、金融、信息通信等领域企业率先走出去，按照公平原则参与国际竞争，共同开拓国际市场，构建跨境产业链体系。鼓励中国企业积极参与他国能力建设，帮助发展中国家发展远程教育、远程医疗、电子商务等行业，促进这些国家的社会发展。

八、加强全球信息基础设施建设和保护

共同推动全球信息基础设施建设，铺就信息畅通之路。推动与周边及其它国家信息基础设施互联互通和“一带一路”建设,让更多国家和人民共享互联网带来的发展机遇。

加强国际合作，提升保护关键信息基础设施的意识，推动建立政府、行业与企业的网络安全信息有序共享机制，加强关键信息基础设施及其重要数据的安全防护。

推动各国就关键信息基础设施保护达成共识,制定关键信息基础设施保护的合作措施，加强关键信息基础设施保护的立法、经验和技术交流。

推动加强各国在预警防范、应急响应、技术创新、标准规范、信息共享等方面合作，提高网络风险的防范和应对能力。

九、促进网络文化交流互鉴

推动各国开展网络文化合作，让互联网充分展示各国各民族的文明成果，成为文化交流、文化互鉴的平台，增进各国人民情感交流、心灵沟通。以动漫游戏产业为重点领域之一，务实开展与“一带一路”沿线国家的文化合作，鼓励中国企业充分依托当地文化资源，提供差异化网络文化产品和服务。利用国内外网络文化博览交易平台，推动中国网络文化产品走出去。支持中国企业参加国际重要网络文化展会。推动网络文化企业海外落地。

结束语

21 世纪是网络和信息化的时代。在新的历史起点上，中国提出建设网络强国的宏伟目标，这是落实“四个全面”战略布局的重要举措，是实现“两个一百年”奋斗目标和中华民族伟大复兴中国梦的必然选择。中国始终是网络空间的建设者、维护者和贡献者。中国网信事业的发展不仅将造福中国人民，也将是对全球互联网安全和发展的贡献。

中国在推进建设网络强国战略部署的同时，将秉持以合作共赢为核心的新型国际关系理念，致力于与国际社会携起手来，加强沟通交流，深化互利合作，构建合作新伙伴，同心打造人类命运共同体，为建设一个安全、稳定、繁荣的网络空间作出更大贡献。

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

工业和信息化部关于开展互联网信息服务备案用户真实身份信息电子化核验试点工作的通知

（工信部信管函〔2019〕87号）

各省、自治区、直辖市通信管理局，中国互联网协会、国家计算机网络应急技术处理协调中心，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，网络接入服务提供者：

根据《中华人民共和国网络安全法》《中华人民共和国电信条例》《互联网信息服务管理办法》《工业和信息化部关于进一步落实网站备案信息真实性核验工作方案（试行）》（工信部电管〔2010〕64号，以下简称64号文）等规定，为切实减轻企业负担，进一步提升互联网信息服务（ICP）备案主体真实身份信息准确率，实现“数据多跑路，群众少跑腿”，我部决定于2019年4月1日至2019年12月31日开展ICP备案主体真实身份信息电子化核验试点工作。有关事项通知如下：

一、试点工作内容

（一）ICP备案主体身份信息电子化采集

参与试点的网络接入服务提供者可采用“人脸识别”“唇语识别”“动作识别”等技术手段，采集确认ICP备案主体真实身份信息，并与其提供的主体身份证件、权威库留存的主体身份证件进行交叉比对。验证一致后，向“工业信息化部ICP/IP地址/域名备案管理系统”提交相关信息。

电子化采集ICP备案主体真实身份信息，准确率不低于99.95%。

通过电子化采集上传的图像，不再要求其提供以幕布为背景的图像。

（二）《ICP备案信息真实性核验单》电子化提交

参与试点的网络接入服务提供者应按照《ICP备案信息真实性核验单》，认真核验ICP备案主体真实身份信息，核验一致后按格式生成《ICP备案信息真实性核验单》，并向“工业和信息化部ICP/IP地址/域名信息备案管理系统”提交相关信息。

电子化采集《ICP备案信息真实性核验单》相关信息，准确率达到100%。提交电子化《ICP备案信息真实性核验单》即表示网络接入服务提供者已履行ICP备案主体真实身份信息核验义务，无须单位盖章，不再提交纸质《ICP备案信息真实性核验单》。

二、参与试点单位条件

参与试点的网络接入服务提供者应具备以下条件：

（一）取得电信主管部门颁发的增值电信业务许可，业务种类包括互联网数据中心业务、互联网接入服务业务、内容分发网络业务等。

（二）具备采集确认 ICP 备案主体真实身份信息的技术能力。

（三）具备与主体信息权威库（统一社会信用代码、个人身份证件库等）信息比对的技术能力。

三、试点工作安排

（一）申请阶段（2019 年 4 月 1 日至 4 月 15 日）。申请参与试点工作的网络接入服务提供者向属地通信管理局提交申请表（详见附件）。

（二）审查阶段（2019 年 4 月 16 日至 5 月 15 日）。各地通信管理局对属地申请参与试点工作的网络接入服务提供者进行审核汇总，报送至部（信息通信管理局）。部（信息通信管理局）组织相关机构对申请参与试点工作的网络接入服务提供者的技术能力进行评估，确定试点单位名单。

（三）试点运行阶段（2019 年 5 月 16 日至 2019 年 12 月 31 日）。参与试点工作的网络接入服务提供者向“工业和信息化部 ICP/IP 地址/域名信息备案管理系统”提交电子化采集的 ICP 备案主体图像和电子化《ICP 备案信息真实性核验单》。

（四）总结评估阶段（2019 年 12 月 31 日至 2020 年 1 月 31 日）。各地通信管理局组织属地参与试点工作的网络接入服务提供者开展评估总结工作，并报至部（信息通信管理局）。

四、工作要求

（一）周密部署，加强指导。各相关单位要严格落实主体责任，依据文件要求周密部署开展工作。各地通信管理局要和参与试点工作的网络接入服务提供者建立协调沟通机制，及时发现处理试点工作存在的问题，切实提高 ICP 备案工作效率，提升 ICP 备案主体真实身份信息数据准确率。

（二）强化监督，严格问责。各地通信管理局要督促网络接入服务提供者严格落实 64 号文和试点工作要求。不具备电子化核验技术能力的网络接入服务提供者，要求其严格落实 64 号文现场核验要求。发现参与试点的网络接入服务提供者故意提供错误或虚假信息

的，立即取消其试点资格并进行处罚。

（三）加强保障，跟踪进展。各地通信管理局要督促参与试点的网络接入服务提供者不断完善技术能力和安全保障措施，确保试点工作平稳有序进行。各相关单位应建立信息报告制度，及时报送各项工作进展，我部将通过《工业和信息化部 ICP 备案工作情况月通报》予以通报。

工业和信息化部

2019 年 3 月 27 日

附件

互联网信息服务备案主体真实身份信息电子化核验试点工作申请表

企业名称			
企业注册地址			
取得电信业务经营许可情况			
联系人姓名		联系人手机号	
联系人邮箱			
承诺内容	本单位自愿报名参加互联网信息服务备案主体真实身份信息电子化核验试点工作，服从电信主管部门安排，严格按照试点工作业务流程开展工作，主动反映沟通试点工作中遇到的问题， 如违反电信主管部门要求，自愿接受电信主管部门的相关管理措施。 企业法定代表人（签名）：		

	（企业盖章） 日期： 本单位自愿报名参加互联网信息服务备案主体真实身份信息电子化核验试点工作，服从电信主管部门安排，严格按照试点工作业务流程开展工作，主动反映沟通试点工作中遇到的问题， 如违反电信主管部门要求，自愿接受电信主管部门的相关管理措施。 企业法定代表人（签名）： （企业盖章） 本单位自愿报名参加互联网信息服务备案主体真实身份信息电子化核验试点工作，服从电信主管部门安排，严格按照试点工作业务流程开展工作，主动反映沟通试点工作中遇到的问题， 如违反电信主管部门要求，自愿接受电信主管部门的相关管理措施。 企业法定代表人（签名）： （企业盖章）

工业和信息化部印发《工业和信息化部关于进一步落实网站备案信息真实性核验工作方案（试行）》的通知

（工信部电管函[2010]64号）

各省、自治区、直辖市通信管理局，国家计算机网络应急技术处理协调中心、中国互联网络信息中心、中国互联网协会、中国电信集团公司、中国移动集团公司、中国联合网络通信集团有限公司，相关接入服务单位：

为贯彻落实《工业和信息化部关于进一步深入整治手机淫秽色情专项行动工作方案》（工信部电管〔2009〕672号文件）的要求，深入开展依法打击手机淫秽色情专项行动，净化互联网络环境，加强对网站备案信息的核查，进一步提高网站备案信息准确率，充分发挥网站备案管理的网站主办者溯源和接入地溯源作用，工业和信息化部在广泛征求各方意见的基础上，制定了《工业和信息化部关于进一步落实网站备案信息真实性核验工作方案（试行）》，现印发给你们，请结合实际工作认真贯彻执行。

二〇一〇年二月八日

工业和信息化部关于进一步落实网站备案信息真实性核验工作方案（试行）

为切实保证网站备案信息的真实性，落实《工业和信息化部关于进一步深入整治手机淫秽色情专项行动工作方案》中的要求：“基础电信企业和各接入服务商在向通信管理局提交网站申请备案之前，要对主办者身份信息当面核验、留存有效证件复印件，要对网站主体信息、联系方式和接入信息等进行审查”。依据《互联网信息服务管理办法》（国务院令第292号）、《非经营性互联网信息服务备案管理办法》（信息产业部令第33号）的相关规定，制定网站备案信息真实性核验工作方案。

一、核验内容

接入服务单位根据相关网站的委托代为履行备案、备案变更等手续时，应对网站主办者提交的主体信息、联系方式、网站信息，以及本单位提交的接入信息的真实性进行核验。

1.网站主办者（主体）信息

网站主办者是指互联网信息服务提供者，包括单位和个人两类。

（1）网站主办者为单位，核验证件为：

如网站主办者为机关、事业单位、社会团体，组织机构代码证书原件为核验其单位资质的第一证件，在没有组织机构代码证书的情况下，可核验事业法人证书或社团法人证书等原件。

如网站主办者为企业，核验工商营业执照或组织机构代码证书等原件。

如网站主办者为军队，核验军队代号证书原件。

网站负责人的个人证件：如网站负责人为中国公民，身份证原件为核验其身份的第一证件，在没有身份证的情况下，可核验户口簿、军官证、台胞证等原件；如网站负责人非中国公民，则核验其护照原件。

（2）网站主办者为个人，核验证件为：

如网站主办者为中国公民，身份证原件为核验其身份的第一证件，在没有身份证的情况下，可核验户口簿、军官证、台胞证等原件。

如网站主办者非中国公民，则核验其护照原件。

（3）网站负责人的定义：若网站主办者为单位，网站负责人是指法定代表人或单位委派具体负责网站的部门负责人；若网站主办者为个人，网站负责人为其本人。

2.联系方式

如网站主办者为单位，联系方式是指网站负责人手机号码、办公电话、电子邮箱、通信地址；如网站主办者为个人，联系方式是指网站负责人手机号码、办公电话或住宅电话、电子邮箱、通信地址。

3.网站信息

网站名称、网站域名、涉及需前置审批或专项审批内容、网站服务内容/项目。

4.接入信息

接入服务提供者名称、接入方式、服务器放置地点、网站 IP 地址。

二、核验、审核、核查规程

（一）备案信息真实性责任主体

接入服务单位根据相关网站的委托代为履行备案、备案变更等手续时，核验主体为接入服务单位，包括：基础电信企业省分公司（含市、县级分公司）、互联网接入服务单位

（IDC、ISP）、公益性互联单位等。

审核主体为各省、自治区、直辖市通信管理局。

核查主体为工业和信息化部（委托国家互联网备案管理支撑中心，以下简称“备案中心”）。

（二）备案信息真实性核验、审核、核查规程

网站备案信息真实性核验、审核工作流程图见附件。

1.接入服务单位网站备案核验规程

（1）网站主办者登录接入服务单位备案系统录入网站备案信息。

（2）接入服务单位受理网站主办者提交信息后，对主体信息、联系方式等信息进行预核验：初步判定主体信息是否真实，通过电话、邮件等途径核验联系方式是否正确。预核验后，接入服务单位应向网站主办者发送现场核验通知或信息退回的短信提示：“您提交的网站备案信息已通过预核验，请在1个月内由网站负责人本人携带有关证件原件到我单位备案现场办理核验手续”或“您提交的网站备案信息未通过预核验，请修改后重新提交”。预核验工作必须在主办者提交备案信息后5个工作日内完成。

（3）网站主办者接到通知后，由网站负责人本人携带核验所需证件原件、材料到接入服务单位备案现场办理核验手续。

（4）接入服务单位在本单位备案现场采集并留存网站负责人彩色正面免冠照（电子照片规格：800×600像素）。备案中心统一制作、提供带有标识的幕布作为拍照背景，照片应显示拍照时间和背景标识。

（5）接入服务单位备案人员利用公安、质检、工商等相关部门提供的居民身份证、组织机构代码证、工商营业执照等信息源，核验网站主办者提供证件原件的真实性。同时通过网站负责人身份证原件核验身份证与当事人是否一致。核验无误，留存身份证明和单位有效证件复印件。

接入服务单位备案人员登录本单位备案系统，依据证件原件内容对网站主办者网上提交的主体信息进行核验：核验证件持有者、证件类型、证件内容与备案系统中录入的网站备案信息是否完全一致，不一致不予受理；依据网站主办者提交的域名证书或域名注册机构网站公共查询信息，核验网站域名所有者与网站主办者身份的一致性，不一致不予受理；依据本单位对网站的实际接入情况，准确录入网站备案接入信息各项内容。

（6）若核验无误，接入服务单位备案人员填写统一格式的《网站备案信息真实性核验单》（备案中心负责制订《网站备案信息真实性核验单》格式）；若发现备案信息有误，现场核实修改，并在《网站备案信息真实性核验单》中进行记录。《网站备案信息真实性核验单》一式两份：一份接入服务单位留存，一份上报网站主体所在地通信管理局，加盖接入服务单位公章。网站主办者和接入服务单位同时签订信息安全管理协议书。

（7）在确认备案信息全部核验无误后，接入服务单位通过本单位备案系统向主体所在地通信管理局备案系统提交网站备案信息，并提交《网站备案信息真实性核验单》纸制原件、传真件或电子扫描件。

2.省通信管理局审核规程

各省、自治区、直辖市通信管理局登录省局备案系统，在二十个工作日内对接入服务单位提交备案信息进行审核。审核合格下发网站备案号，接入服务单位实施网站接入；不合格将备案信息退回接入服务单位系统，由接入服务单位重新核验。

3.备案中心核查规程

（1）备案中心受工业和信息化部委托，建设网站备案信息校验平台，对各通信管理局提交网站备案信息中的身份证信息进行全量自动核查。结合人工电话抽查，每月对备案系统提交的网站备案信息进行准确性核查和抽样评估并反馈情况。

（2）备案中心每季度对部备案系统中存量网站备案信息准确率、备案率分省分接入商进行核查和抽样评估并反馈情况。

三、工作要求

（一）接入服务单位核验工作要求

1.组织保障和制度完善要求

各接入服务单位应在2010年2月底前设立现场核验网站备案信息部门,专门负责网站备案信息真实性核验工作，并实行单位领导负责制。应建立本单位的备案业务规范，备案工作考核制度。明确备案人员的工作责任，对备案人员业务能力实行年度考核，将日常备案工作质量作为考核的重要指标。

各接入服务单位应在2010年3月底前正式实施网站备案信息当面核验,并将工作开展情况报许可证发证机关和单位注册所在地通信管理局。

基础电信企业应在2010年4月份对租用本单位电信资源从事接入业务的接入服务单位

是否设立当面核验人员、履行当面核验备案信息的情况进行检查，对未履行当面核验责任的，不得为其提供电信资源。

2.业务明示要求

接入服务单位在业务经营中应向网站主办者明示开办网站要依法办理备案手续、网站备案流程、需提供的证件、材料清单及网站备案有关注意事项。

3.业务合同内容要求

接入服务单位应在与网站主办者签订业务合同中，明文要求：“依据《非经营性互联网备案管理办法》第二十三条规定，如备案信息不真实，将关闭网站并注销备案。请您承诺并确认：您提交的所有备案信息真实有效，当您的备案信息发生变化时请及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，我公司有权依法对接入网站进行关闭处理。”双方签字、单位盖章确认。

4.信息安全管理责任要求

接入服务单位建立网站主办者资料档案，妥善保管核验过程中获取的网站主办者证件信息、照片信息、《网站备案信息真实性核验单》、与网站主办者签署的各项协议，保证信息不泄露，承担对网站主办者提交材料的信息安全保密管理责任。上述资料至少留存5年以上，以备通信行业主管部门依法进行检查。

5.网站备案信息更新要求

接入服务单位应做好日常回访核查工作，确保网站备案信息变更后，网站主办者及时更新主体信息、联系方式、网站信息。同时接入服务单位应根据网站接入变化情况，及时更新接入信息，并配合主管部门做好网站备案信息真实性核查工作。因未开展日常回访核查工作导致接入网站备案信息不准确的接入服务单位，主管部门依法对其进行处罚。

6.存量网站备案信息核验要求

对备案信息真实性当面核验工作正式启动前接入的网站，各接入服务单位要在2010年2月底前制定备案信息真实性核验工作详细计划，报许可证发证机关和单位注册所在地通信管理局，并在2010年9月底前完成全部网站的备案信息真实性核验。

（二）省通信管理局审核工作要求

1.做好日常审核工作

各通信管理局应做好日常网站备案信息真实性审核工作，保证对重点信息（营业执照、

身份证等）的逐一细致审核。二期备案系统升级改造后可由各通信管理局审核人员用口令登录接入服务单位系统抽检审核证件原件，同时检查接入服务单位上交的《网站备案信息真实性核验单》。

2.检查“当面核验”工作开展情况

各通信管理局对接入服务单位当面核验网站备案信息的部门设立和工作制度完善情况进行指导和检查。根据接入服务单位保存的真实性核验证明材料，对接入服务单位“当面核验”工作的开展情况、接入服务单位提交备案信息的准确性进行定期检查或不定期抽查，对发现未执行“当面核验”或提供虚假信息的，应严肃处理。同时将日常检查考核结果作为许可证年检重要参考。

（三）备案中心核查工作要求

1.新增网站备案信息核查

备案中心每月对新提交的网站备案信息进行准确性抽查。对备案主体信息中身份证、组织机构代码证等信息进行重点抽查核查。

2.存量网站备案信息核查

备案中心按季度对系统存量网站备案信息进行准确性核查，对各接入服务单位真实性核验网站备案信息工作开展情况、完成进度、工作质量进行核查和抽查评估。

3.制定核查标准和监督评估办法

备案中心根据工业和信息化部的委托，适时制订、细化、完善网站备案信息核查标准和监督评估办法，并向各通信管理局、接入服务单位发布。

4.加强对工作开展情况的督导、统计

备案中心根据工业和信息化部的委托，对各单位落实网站备案信息真实性核验工作开展情况进行指导帮助和监督评估。加强对各单位落实网站备案信息真实性核验工作情况的分类统计，开展对各地通信管理局行政处罚情况汇总等工作。

5.开展网站备案业务培训

备案中心根据工业和信息化部的委托，编写、制订网站备案培训资料，组织开展面向各接入服务单位的全国性网站备案培训工作，对应掌握的网站备案相关政策法规、业务知识进行统一讲解。

四、问责

各省、自治区、直辖市通信管理局根据属地化管理原则，对未按《工业和信息化部关于进一步深入整治手机淫秽色情专项行动工作方案》中提出的“对网站主办者身份信息当面核验、留存有效证件复印件”要求开展工作，未认真开展网站备案信息真实性核验工作，提交不真实网站备案信息的接入服务单位，依据《非经营性互联网信息服务备案管理办法》第十条和第二十四条的规定依法处罚，责令限期改正。

附件：网站备案信息真实性核验、审核工作流程图 （略）

工业和信息化部关于印发《工业互联网平台建设及推广指南》和《工业互联网平台评价方法》的通知

（工信部信软〔2018〕126号）

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门：

现将《工业互联网平台建设及推广指南》和《工业互联网平台评价方法》印发给你们，请认真贯彻执行。

附件1：工业互联网平台建设及推广指南

附件2：工业互联网平台评价方法

工业和信息化部

2018年7月9日

附件1：

工业互联网平台建设及推广指南

工业互联网平台是面向制造业数字化、网络化、智能化需求，构建基于云平台的海量数据采集、汇聚、分析服务体系，支撑制造资源泛在连接、弹性供给、高效配置。为贯彻落实《国务院关于深化“互联网＋先进制造业”发展工业互联网的指导意见》，加快发展工业互联网平台，制定本指南。

一、总体要求

深入贯彻落实党的十九大和十九届二中、三中全会精神，以习近平新时代中国特色社会主义思想为指导，坚持新发展理念，聚焦工业互联网平台发展，以平台标准为引领，坚持建平台和用平台双轮驱动，打造平台生态体系，优化平台监管环境，加快培育平台新技术、新产品、新模式、新业态，有力支撑制造强国和网络强国建设。

到2020年，培育10家左右的跨行业跨领域工业互联网平台和一批面向特定行业、特定区域的企业级工业互联网平台，工业APP大规模开发应用体系基本形成，重点工业设备上云取得重大突破，遴选一批工业互联网试点示范（平台方向）项目，建成平台试验测试和公共服务体系，工业互联网平台生态初步形成。

二、制定工业互联网平台标准

（一）建立工业互联网平台标准体系。制定工业互联网平台参考架构、技术框架、评价指标等基础共性标准。组织推进边缘计算、异构协议兼容适配、工业微服务框架、平台数据管理、平台开放接口、应用和数据迁移、平台安全等关键技术标准制定，面向特定行业制定形成一批平台应用标准。

（二）推动形成平台标准制定与推广机制。充分发挥企业、高校、科研院所、联盟、行业协会作用，推动国家标准、行业标准和团体标准的制定与推广。建设标准管理服务平台，开发标准符合性验证工具及解决方案，在重点行业、重点区域开展标准宣贯培训。

（三）推动平台标准国际对接。建立与国际产业联盟、标准化组织的对标机制，等同采纳国际标准，加快国际标准的国内转化。支持标准化机构、重点企业主导或实质参与国际标准制定。

三、培育工业互联网平台

（四）遴选 10 家左右的跨行业跨领域工业互联网平台。制定工业互联网平台评价方法，在地方普遍发展工业互联网平台的基础上，分期分批遴选跨行业跨领域平台，加强跟踪评价和动态调整。组织开展工业互联网试点示范（平台方向）、应用现场会，推动平台在重点行业和区域落地，支持跨行业跨领域平台拓展国际市场。

（五）发展一批面向特定行业、特定区域的企业级工业互联网平台。制定工业互联网平台服务能力规范，支持协会联盟等开展平台能力成熟度评价，发布重点行业工业互联网平台推荐名录。鼓励地方建设工业互联网平台省级制造业创新中心，推动平台在“块状经济”产业集聚区落地。

（六）提升工业互联网平台设备管理能力。支持建设工业设备协议开放开源社区，引导设备厂商、自动化企业开放设备协议、数据格式、通信接口等源代码， 形成工业设备数据采集案例库和工具箱。组织开展边缘计算技术测试与应用验证，推动基于工业现场数据的实时智能分析与优化。

（七）加速工业机理模型开发与平台部署。鼓励平台整合高校、科研院所等各方资源，推动重点行业基础共性技术的模型化、组件化、软件化与开放共享，促进基于工业互联网平台的工业知识沉淀、传播、复用与价值创造。

（八）强化工业互联网平台应用开发能力。支持平台建设多类开发语言、建模工具、

图形化编程环境，开发平台化、组件化的行业解决方案软件包，推动面向场景的多功能、高灵活、预集成平台方案应用部署。

（九）打造面向工业场景的海量工业 APP。组织研制工业 APP 参考架构、通用术语、分类准则等标准。编制和滚动修订基础共性工业 APP 需求目录，支持平台联合各方建设基础共性和行业通用工业 APP 及微服务资源池。鼓励第三方建设工业 APP 研发协同平台和交易平台，推动工业 APP 交易。

四、推广工业互联网平台

（十）实施工业设备上云“领跑者”计划。制定分行业、分领域重点工业设备数据云端迁移指南，推动工业窑炉、工业锅炉、石油化工设备等高耗能流程行业设备，柴油发动机、大中型电机、大型空压机等通用动力设备，风电、光伏等新能源设备，工程机械、数控机床等智能化设备上云用云，提高设备运行效率和可靠性，降低资源能源消耗和维修成本。鼓励平台在线发布核心设备运行绩效榜单和最佳工艺方案，引导企业通过对标优化设备运行管理能力。

（十一）推动企业业务系统上云。鼓励龙头企业面向行业开放共享业务系统，带动产业链上下游企业开展协同设计和协同供应链管理。鼓励地方通过创新券、服务券等方式加大企业上云支持力度，发挥中小企业公共服务平台、小型微型企业创业创新基地作用，降低中小企业平台应用门槛。

（十二）培育工业互联网平台应用新模式。组织开展工业互联网试点示范（平台方向），培育协同设计、协同供应链管理、产品全生命周期管理、供应链金融等平台应用新模式。组织制定工业互联网平台应用指南，明确平台应用的咨询、实施、评估、培训、采信等全流程方法体系。

五、建设工业互联网平台生态

（十三）建设工业互联网平台试验测试体系。以测带建、以测促用，支持建设一批面向跨行业跨领域、特定区域和特定行业的试验测试环境，以及一批面向特定场景的测试床，开展技术成熟度、功能完整性、协议兼容性、数据安全性等试验测试。

（十四）建设工业互联网平台开发者社区。支持协会联盟联合跨行业跨领域平台建设开发者社区，推动平台开放开发工具、知识组件、算法组件等工具包（SDK）和应用程序编程接口（API），构建工业 APP 开发生态。指导开发者社区建立人才培训、认证、评价

体系，组织开展开发者创业创新大赛，加快工业 APP 开发者人才队伍建设。

（十五）建设工业互联网平台新型服务体系。探索基于平台的知识产权激励和保护机制，创建工业互联网平台知识交易环境。构建基于平台的制造业新型认证服务体系，推动建立线上企业资质、产品质量和服务能力认证新体系。建设工业互联网平台基础及创新技术服务平台，推动资源库建设与技术成果交易。

六、加强工业互联网平台管理

（十六）推动平台间数据与服务互联互通。制定工业互联网平台互联互通规范，构建公平、有序、开放的平台发展环境。制定发布工业互联网平台数据迁移行业准则，实现不同平台间工业数据的自由传输迁移。支持协会联盟制定软件跨平台调用标准，推动工业模型、微服务组件、工业 APP 在不同平台间可部署、可调用、可订阅。

（十七）开展平台运营分析与动态监测。搭建监测分析服务平台，加强与工业互联网平台运营数据共享，实时、动态监测工业互联网平台发展情况。发布工业 APP 订阅榜、平台用户地图等榜单，开发细分行业产能分布数字地图。加强工业大数据管理与新技术应用，推进平台间数据安全流动、可信交易、汇聚共享和服务增值。

（十八）完善平台安全保障体系。制定完善工业信息安全管理等政策法规，明确安全防护要求。建设国家工业信息安全综合保障平台，实时分析平台安全态势。强化企业平台安全主体责任，引导平台强化安全防护意识，提升漏洞发现、安全防护和应急处置能力。

附件 2：

工业互联网平台评价方法

为规范和促进我国工业互联网平台发展，支撑开展工业互联网平台评价与遴选，制定本方法。工业互联网平台评价重点包括平台基础共性能力要求、特定行业平台能力要求、特定领域平台能力要求、特定区域平台能力要求、跨行业跨领域平台能力要求五个部分。

一、基础共性能力要求

工业互联网平台基础共性能力要求包括平台资源管理、应用服务等工业操作系统能力，以及平台基础技术、投入产出效益共四个方面。

（一）平台资源管理能力

1.工业设备管理。兼容多类工业通信协议，可实现生产装备、装置和工业产品的数据采集。部署各类终端边缘计算模块，可实现工业设备数据实时处理。适配主流工业控制系统，可实现参数配置、功能设定、维护管理等设备管理操作。

2.软件应用管理。可基于云计算服务架构，提供研发、采购、生产、营销、管理和服务等工业软件，提供工业软件集成适配接口。可基于平台即服务架构，提供面向各类工业场景的机理模型、微服务组件和工业 APP。具备各类软件应用及工业 APP 的搜索、认证、交易、运行、维护等管理能力。

3.用户与开发者管理。具备多租户权限管理、用户需求响应、交易支付等多类用户管理功能。建有开发者社区，能够集聚各类开发者，并提供应用开发、测试、部署和发布的各类服务和管理功能。

4.数据资源管理。具备海量工业数据资源的存储与管理功能，部署多类结构化、非结构化数据管理系统，提供工业数据的存储、编目、索引、去重、合并及质量评估等管理功能。

（二）平台应用服务能力

1.存储计算服务。具备云计算运行环境，部署主流数据库系统，能够为用户提供可灵活调度的计算、存储和网络服务，满足海量工业数据的高并发处理需求，且积累存储一定规模的工业数据。

2.应用开发服务。提供多类开发语言、开发框架和开发工具，提供通用建模分析算法，能够支撑数据模型及软件应用的快速开发，满足多行业多场景开发需求。

3.平台间调用服务。支持工业数据在不同 IaaS 平台间的自由迁移。支持工业软件、机理模型、微服务、工业 APP 在不同 PaaS 平台间的部署、调用和订阅。

4.安全防护服务。部署安全防护功能模块或组件，建立安全防护机制，确保平台数据、应用安全。

5.新技术应用服务。具备新技术应用探索能力，开展人工智能、区块链、VR/AR/MR 等新技术应用。

（三）平台基础技术能力

1.平台架构设计。具有完整的云计算架构，能够基于公有云、私有云或混合云提供服务。

2.平台关键技术。具有设备协议兼容、边缘计算、异构数据融合、工业大数据分析、工业应用软件开发与部署等关键技术能力。

（四）平台投入产出能力

1.平台研发投入。具备对平台的可持续投入能力，财务状况、研发投入合理。

2.平台产出效益。能够依托各类服务及解决方案，为平台企业创造良好经济效益

3.平台应用效果。具有良好的应用效果，能够基于平台应用带动制造企业提质增效。

4.平台质量审计。具有明确的运行安全和质量审计机制和能力，以降低由平台运营的潜在风险引起的损失。

二、特定行业平台能力要求

在工业互联网平台基础共性能力基础上，特定行业平台在设备接入、软件部署和用户覆盖三个方面具有额外要求。

（一）行业设备接入能力

平台在特定行业具有设备规模接入能力，连接不少于一定数量特定行业工业设备（离散行业）或不少于一定数量特定行业工艺流程数据采集点（流程行业）。

（二）行业软件部署能力

平台在特定行业具有工业知识经验的沉淀、转化与复用能力，提供不少于一定数量行业软件集成接口、特定行业机理模型、微服务组件，以及不少于一定数量特定行业工业 APP。

（三）行业用户覆盖能力

平台在特定行业具有规模化应用能力，覆盖不少于一定数量特定行业企业用户或不少于一定比例特定行业企业。

三、特定领域平台能力要求

在工业互联网平台基础共性能力基础上，特定领域平台在关键数据打通、关键领域优化构建两个方面具有额外要求。

（一）关键数据打通能力

特定领域平台能够实现研发设计、物料采购、生产制造、运营管理、仓储物流、产品服务等产品全生命周期，供应链企业、协作企业、市场用户、外部开发者等各主体数据的打通，实现全流程的数据集成、开发、利用。

（二）关键领域优化能力

特定领域平台能够实现在某一关键领域的应用开发与优化服务，提升关键环节生产效率与产品质量。如协同设计、供应链管理、智能排产、设备预测性维护、产品质量智能检测、仓储与物流优化等。

四、特定区域平台能力要求

在工业互联网平台基础共性能力基础上，特定区域平台在地方合作、资源协同、规模推广三个方面具有额外要求。

（一）区域地方合作能力

平台在特定区域（工业园区或产业集聚区）落地，在该地具有注册实体，与地方政府签订合作协议，具备在地方长期开发投入、运营服务能力。

（二）区域资源协同能力

平台具有面向特定区域产业转型升级共性需求的服务能力，能够促进区域企业信息共享与资源集聚，带动区域企业协同发展。

（三）区域规模推广能力

平台具有特定区域企业的规模覆盖能力，为不少于一定数量特定区域企业或不低于一定比例特定区域企业提供服务。

五、跨行业跨领域平台能力要求

在工业互联网平台基础共性能力、特定行业能力、特定区域能力、特定领域能力基础

上，跨行业跨领域平台要求包括如下五个方面。

（一）平台跨行业能力

平台覆盖不少于一定数量特定行业：

每个行业连接不少于一定数量行业设备（离散行业）或不少于一定数量行业工艺流程数据采集点（流程行业）。

每个行业部署不少于一定数量行业机理模型、微服务组件，以及不少于一定数量行业工业 APP。

每个行业覆盖不少于一定数量企业用户或不少于一定比例行业企业。

（二）平台跨领域能力

平台覆盖不少于一定数量特定领域：

每个领域之间能够实现不同环节、不同主体的数据打通、集成与共享。

每个领域具有不少于一定数量面向该领域（关键环节）的工业机理模型、微服务组件或工业 APP。

（三）平台跨区域能力

平台覆盖不少于一定数量特定区域：

平台在全国（华北、华东、华南、华中、西北、东北）主要区域注册不低于一定数量运营实体，负责平台在当地区域的运营推广。每个区域具有不少于一定数量特定区域企业用户或为不低于一定比例的特定区域企业提供服务。

（四）平台开放运营能力

1.平台具备独立运营能力。具有独立法人实体或完整组织架构的集团独立部门，人员规模不少于一定规模。

2.平台具备开放运营能力。建立产学研用长期合作机制，建有开发者社区，且第三方开发者占平台开发者总数比例不低于一定比例。

（五）平台安全可靠能力

1.工控系统安全可靠。在平台中建立工控系统安全防护机制，主动防护漏洞危害与病毒风险。

2.关键零部件安全可靠。在平台边缘计算或人工智能应用中，具备关键零部件的安全可靠能力。

3.软件应用安全可靠。平台创新开发一定数量工业机理模型、微服务组件或工业 APP。

工业和信息化部关于印发《工业互联网网络建设及推广指南》的通知

（工信部信管〔2018〕301号）

各省、自治区、直辖市及计划单列市工业和信息化主管部门、通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，各有关单位：

现将《工业互联网网络建设及推广指南》印发给你们，请认真贯彻执行。

工业和信息化部

2018年12月29日

工业互联网网络建设及推广指南

工业互联网网络是构建工业环境下人、机、物全面互联的关键基础设施，通过工业互联网网络可以实现工业研发、设计、生产、销售、管理、服务等产业全要素的泛在互联，对于促进工业数据的开放流动与深度融合、推动工业资源的优化集成与高效配置、支撑工业应用的创新升级与推广普及具有重要意义。为贯彻落实《国务院关于深化“互联网＋先进制造业”发展工业互联网的指导意见》，加快工业互联网网络基础设施建设及推广，制定本指南。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的十九大和十九届二中、三中全会精神，坚持新发展理念，坚持高质量发展，以加快企业外网络和企业内网络建设与改造为主线，以构筑支撑工业全要素、全产业链、全价值链互联互通的网络基础设施为目标，以企业网络应用创新和传统产业升级为牵引，着力构建网络标准体系、加强技术引导，着力打造工业互联网标杆网络、创新网络应用，着力建设标识解析体系、拓展标识应用，着力完善网络创新环境，规范发展秩序，加快培育网络新技术、新产品、新模式、新业态，有力支撑制造强国和网络强国建设。

（二）工作目标

到2020年，形成相对完善的工业互联网网络顶层设计，初步建成工业互联网基础设施和技术产业体系。一是建设满足试验和商用需求的工业互联网企业外网标杆网络，初步建成适用于工业互联网高可靠、广覆盖、大带宽、可定制的支持互联网协议第六版（IPv6）的企业外网络基础设施；建设一批工业互联网企业内网标杆网络，形成企业内网络建设和改造的典型模式，完成100个以上企业内网络建设和升级。二是建成集成网络技术创新、标准研制、测试认证、应用示范、产业促进、国际合作等功能的开放公共服务平台；建成一批关键技术和重点行业的工业互联网网络实验环境，建设20个以上网络技术创新和行业应用测试床，初步形成工业互联网网络创新基地。三是形成先进、系统的工业互联网网络技术体系和标准体系，在网络领域建成一批工业互联网应用创新示范项目，建立工业互联网网络改造评估认证机制，构建适应工业互联网发展的网络技术产业生态。四是初步构建工业互联网标识解析体系，建设一批面向行业或区域的标识解析二级节点以及公共递归节点，制定并完善标识注册和解析等管理办法，标识注册量超过20亿。

二、制定工业互联网网络标准

工业和信息化部会同国家标准化管理机构加强工业互联网网络标准体系的顶层设计和统筹协调，充分发挥工业互联网产业联盟及工业、电子信息、通信等领域标准化机构和行业协会优势，依托企业、科研机构和高校等加快研制工业互联网网络标准。地方工业和信息化主管部门、通信管理部门积极推动工业互联网网络标准在企业中的应用与推广。

（一）建立工业互联网网络标准体系。一是制定工业互联网网络通用需求、网络架构、通信协议、关键接口等总体性标准，时间敏感网络（TSN）、工业无源光网络（PON）、工业软件定义网络（SDN）、无线专网等新型网络技术标准，以及针对垂直行业的特色网络应用技术标准。二是制定工业互联网网络服务标准，进一步规范网络服务提供商的服务流程与服务质量。三是制定企业外网、内网及相互间的互联互通规范，构建公平、有序、开放的网络互联互通环境。

（二）完善标识解析技术标准。一是制定标识解析整体架构、数据管理、分布式注册、可信解析、多源异构信息管理、标识数据互操作等关键技术标准。二是搭建规模性的基础技术创新与试验验证环境，打造安全可控的标签、读写器、中间件等标识存取关键软硬件设备，提供标识注册、标识解析、标识搜索等关键技术测试验证服务。

（三）形成网络标准制定与推广机制。一是在工业互联网领域建立国际标准、国家标准、行业标准、团体标准和企业标准协同推进机制。二是建立一批工业互联网网络新技术标准符合性试验验证系统，开发和推广网络测试测量工具。三是针对重点行业或重点区域，组织开展工业互联网网络标准的宣贯培训。四是支持企业和科研机构积极参与国际标准的研制，建立与国际标准化组织、主流开源项目的对标机制，加快国际标准的国内转化。五是开展网络标准相关专利等知识产权的研究，加强知识产权的布局和保护，提高网络标准专利的知识普及。

三、打造工业互联网标杆网络

以基础电信企业和相关科研机构为主体，加快建设面向商用和面向试验的工业互联网企业外网标杆网络。地方工业和信息化主管部门、通信管理部门组织和支持重点行业、典型企业打造工业互联网企业内网标杆网络。

（四）建设企业外网标杆网络。一是充分利用科研机构既有和正在建设的各类试验网络网络资源，构建面向试验的标杆网络，开展工业互联网网络及应用的研究、试验、验证和试点示范。二是鼓励和支持基础电信企业推进网络技术研究和基础设施建设，开展 IPv6 网络改造，打造面向实际应用的标杆网络，支撑成熟可商用的工业互联网应用。三是打造支撑企业上云时企业网络与云之间的网络接入典型解决方案，形成企业上云“最后一公里”的网络模板。四是支持工业互联网应用从试验平面向实用平面的安全平滑迁移。

（五）打造企业内网标杆网络。一是支持企业建设基于 TSN、工业 PON 等关键网络技术的工业互联网企业内网标杆网络，形成不同网络技术在企业内网部署的参考模板。二是支持企业针对典型行业需求和不同企业规模，建设垂直行业企业内网标杆网络，树立汽车、航空航天、石油化工、机械制造等重点行业的工业互联网企业内网络样板。

四、推动工业互联网网络改造与应用

发挥产业联盟和各行业协会的平台纽带作用，地方工业和信息化主管部门、通信管理部门积极组织协调推动工业企业网络化改造和网络应用创新。

（六）推进传统企业网络化改造。一是支持企业开展针对既有生产设备与系统的网络化二次开发，推动“接口开放、机器上网”，扩大网络覆盖范围和终端连接数量。二是加快企业内网络的 IPv6 改造进程，不断优化企业内网络架构，提升网络服务能力。三是支持企业参照标杆网络开展企业网络建设和改造，将生产性网络的改造纳入中小企业扶持政策范

畴。四是支持高性能、高灵活、高安全隔离的新型企业专线应用，推进企业内外网络互联互通，协调推进基础电信企业与能源、交通、工业制造等重点垂直行业的网络与业务对接，打通企业内外网络之间的信息通道。

（七）开展工业互联网网络应用创新。一是充分发挥企业、高校、科研院所、产业联盟作用，开展基于IPv6、标识解析等网络技术的应用创新，繁荣工业互联网网络上的应用生态。二是开展工业互联网网络应用示范，培育新业态与新模式。三是鼓励企业依托工业互联网网络环境，改造传统生产流程、优化组织模式，提升生产效率，促进产业升级。

五、构建工业互联网标识解析体系

工业和信息化部推动建立工业互联网标识解析管理机制，地方通信管理部门与工业和信息化主管部门加强工作协同，依托相关行业协会、骨干工业企业、信息化服务提供商、基础电信企业、标识研究机构及高等院校加快建设各级服务节点。

（八）建立标识解析管理机制。针对标识注册服务规范和标识解析节点运行要求，制定工业互联网标识解析管理办法,建设一批面向重点行业或区域的二级服务节点运营机构，建立国际根节点、国家顶级节点、二级及以下其他服务节点的建设和运营的统筹协调机制。

（九）建设各级标识解析节点。一是建设和运营国家顶级节点，提供顶级域解析服务，与国内外各主要标识解析系统实现互联互通，形成备案、监测等公共服务能力。二是选择汽车、机械制造、新材料、能源化工、生物医药、高端装备等领域，建设和运营一批标识解析二级节点。

六、拓展工业互联网标识解析应用

地方工业和信息化主管部门、通信管理部门组织和推动典型工业企业、信息化服务提供商、基础电信企业、标识研究机构和高等院校等开展工业互联网标识解析应用创新，加强标识技术产品研发。

（十）推动标识解析集成创新应用。一是加快工业互联网标识解析集成创新，开展基于标识解析服务的关键产品追溯、供应链管理、智能产品全生命周期管理等创新应用，形成一批有较强影响力的工业互联网标识解析先导应用模式。二是建立标识解析服务提供商名录，实现标识解析服务资源池和标识解析应用需求池对接，打通供需对接渠道。

（十一）提升标识解析技术产业能力。一是打造标识解析创新开源社区，汇聚科研机构和企业等的研发资源，加强前沿技术领域共创共享，推进标识解析核心软硬件产品。二

是结合区域性产业特色与资源优势，围绕标识解析产业上下游的关键技术、核心装置、系统软件、集成应用等环节，打造一批具有竞争力的龙头企业，形成聚集基础研究、技术研发、服务支持、应用推广、产业化、教育培训、投融资等各环节的产业生态。

七、创建网络发展环境

以工业互联网产业联盟为依托，加快建设工业互联网网络创新公共服务平台；地方工业和信息化主管部门、通信管理部门组织开展面向先进技术和重点行业的工业互联网网络技术与应用测试床建设。

（十二）建设网络创新公共服务平台。一是依托工业互联网产业联盟，组织各方力量，建设创新领先、开放共享的工业互联网网络创新公共服务平台，实现对工业互联网网络技术创新、标准研制、测试认证、应用示范、产业促进、人才培育、国际合作等方面的全方位支撑。二是强化公共服务平台和产业联盟对中小企业的支持力度，为中小企业与产业链各方合作提供便利条件。三是加强对工业互联网网络和标识解析等核心技术、运营机制、应用模式的培训，组织开展工业互联网网络创新大赛，加快工业互联网网络人才队伍建设。

（十三）建设网络技术与应用测试床。一是支持企业、科研机构、高校，针对 5G、窄带物联网（NB-IoT）、软件定义网络（SDN）、网络虚拟化（NFV）、TSN、边缘计算等新型网络技术，联合建设 10 个以上网络技术测试床，开展基础通用关键技术、标准、设备、解决方案的研制研发、试验测试等工作。二是支持企业、科研机构、高校合作，在汽车、航空航天、石油化工、机械制造等重点行业，建设 10 个以上垂直行业网络化改造和标识解析应用测试床。

八、规范网络发展秩序

工业和信息化部加强工业互联网网络建设与应用相关的网络地址、频谱资源的规划和管理，建立工业互联网网络发展监测评估机制。地方工业和信息化主管部门、通信管理部门指导企业落实网络安全要求，统计报送地方工业互联网网络发展情况；支持工业互联网产业联盟等第三方机构积极开展工业互联网网络发展宣传推广工作。

（十四）加强网络资源管理和安全保障。一是推动在工业互联网领域落实 IPv6 地址编码规划方案，建立工业互联网 IPv6 地址申请、分配、使用、备案管理体制。二是加强频率资源管理和统筹，研究制定工业互联网频率使用指南，做好 5G 系统实验的基站与卫星地球站干扰协调、电台执照许可工作，依法做好工业互联网专用频率的干扰保护。三是指

导相关企业在进行网络化改造的同时落实网络安全标准相关要求,提升标识解析顶级节点,二级节点的安全防护能力。四是进行工业互联网设备进网管理制度研究，组织开展联网设备检测。

（十五）加强网络发展监测和宣传推广。一是探索建立工业互联网网络运行监测体系，逐步开展工业互联网外网和企业内网发展情况的动态监测，定期发布工业互联网网络发展报告。二是组织编制工业互联网网络建设与改造优秀案例，通过组织大型峰会、高峰论坛、现场会、成果发布会、巡讲团等形式，加强对工业互联网网络、标识解析领域相关成果和典型经验的推广，提升产业和企业对工业互联网网络的认知。

工业和信息化部关于印发《无线电干扰投诉和查处工作暂行办法》的通知

（工信部无〔2017〕170号）

各省、自治区、直辖市无线电管理机构，国家无线电监测中心，各相关单位：

为进一步加强无线电干扰投诉和查处工作，规范工作程序，有效维护电波秩序，保护用频设台用户合法权益，根据《中华人民共和国无线电管理条例》和相关行政法规，制定《无线电干扰投诉和查处工作暂行办法》，现予印发。请各相关单位加强人员配备，加大工作力度，认真贯彻执行。

工业和信息化部

2017年7月14日

无线电干扰投诉和查处工作暂行办法

第一条　为进一步加强无线电干扰投诉和查处工作，规范无线电干扰查处工作程序，有效维护电波秩序，保护用频设台用户合法权益，根据《中华人民共和国无线电管理条例》和相关行政法规，并参考国际电信联盟《无线电规则》，制定本办法。

第二条　由国家无线电管理机构负责受理并组织开展的无线电干扰投诉和查处工作，适用本办法。

各省、自治区、直辖市无线电管理机构负责受理并组织开展的无线电干扰投诉和查处工作相关规定，由各地无线电管理机构结合实际另行制定。

第三条　国家无线电管理机构负责受理我国境内短波、卫星业务的干扰投诉，境外无线电主管部门向我国提出的干扰投诉；组织国家无线电监测中心、相关省、自治区、直辖市无线电管理机构和其他有关单位开展无线电干扰的查找和处置；代表国家向境外无线电主管部门提出干扰投诉等工作。

省、自治区、直辖市无线电管理机构及其监测站负责承担国家无线电管理机构下达的查处任务。

国家无线电监测中心负责短波、卫星业务的干扰监测和定位，必要时协助地方无线电

管理机构及其监测站开展干扰逼近查找，协助国家无线电管理机构开展涉外无线电干扰相关工作。

第四条　境内合法使用短波、卫星业务的单位或个人，受到无线电有害干扰时，均可向国家无线电管理机构提出干扰投诉。

境外用户受到可能来自我国的无线电干扰时，可由境外相关无线电主管部门向我国无线电管理机构提出干扰投诉。

第五条　要求干扰保护的频率和台站应具备无线电管理机构颁发的在有效期内的频率使用许可或无线电台执照。受干扰的频率和台站如涉及射电天文、气象雷达站、卫星测控（导航）站、机场等需要电磁环境特殊保护的项目，投诉人还应提交在工程选址前征求并采纳无线电管理机构意见的电磁兼容分析和论证报告。

对于向境外无线电主管部门提出干扰投诉的，投诉人应就受干扰频率和台站履行必要的国际协调或国际登记工作，但国际电信联盟《无线电规则》规定的违规发射干扰投诉除外。

第六条　投诉人应通过邮寄函件、传真等书面方式向国家无线电管理机构提出无线电干扰投诉，同时提交无线电干扰投诉单（见附件 1）。

由于突发影响国家安全等重大无线电干扰，确实来不及提出书面干扰投诉的，可通过电话等方式向国家无线电管理机构口头提出干扰投诉，并在 2 个工作日内补发正式函件。

第七条　投诉人应当在干扰投诉前进行自查，排除由于自身设备故障、用户误操作等内部原因造成的干扰。有条件的用户，还可将疑似的干扰源位置、频谱图等相关信息与无线电干扰投诉单一并提交国家无线电管理机构，并在具体干扰查找过程中为无线电管理机构提供必要的协助。

第八条　接到干扰投诉后，国家无线电管理机构应当及时进行审查。符合投诉要求的，及时向相关单位下达无线电干扰排查任务；不符合投诉要求的，应告知投诉人具体原因；投诉资料不全的，应一次性告知投诉人予以补全。

第九条　对于投诉人未上报疑似干扰源位置的投诉，国家无线电管理机构应组织国家无线电监测中心开展监测定位。国家无线电监测中心将初步定位结果按要求报国家无线电管理机构，由国家无线电管理机构转交干扰所在省、自治区、直辖市无线电管理机构进行后续干扰查处工作。

对于投诉人已上报疑似干扰源位置的投诉，国家无线电管理机构可组织国家无线电监测中心开展定位确认，同时安排干扰所在省、自治区、直辖市无线电管理机构开展后续干扰查处工作。

第十条　对于干扰源在境内的，由干扰所在省、自治区、直辖市无线电管理机构按照《中华人民共和国无线电管理条例》和地方无线电管理有关法规依法查处，在规定期限内填写无线电干扰投诉排查任务回执单（见附件2）报国家无线电管理机构。

第十一条　对于干扰源在境外的，投诉人应按照国际电信联盟《无线电规则》对不同干扰类型的投诉要求，填写违章报告（附录9）或有害干扰报告（附录10），由国家无线电管理机构组织开展对外干扰投诉工作。

第十二条　干扰源可能涉及多个省（区、市）的，由国家无线电管理机构牵头，组织相关省、自治区、直辖市无线电管理机构开展联合查处。

在干扰查处工作中遇特殊情况需要协调的，由相关省、自治区、直辖市无线电管理机构组织开展，必要时可请求国家无线电管理机构予以协助。

第十三条　干扰查处工作中发现涉嫌犯罪行为的，相关省、自治区、直辖市无线电管理机构应将案件线索及时移送公安机关或国家安全机关，配合相关单位开展查处工作，并将处理结果报送国家无线电管理机构。

第十四条　干扰查处结束后，国家无线电管理机构应当将查处情况以书面或电话通知等形式及时告知投诉人。

第十五条　国家无线电管理机构应对历次干扰查处情况进行归档分析，不定期对干扰查处情况进行通报。省、自治区、直辖市无线电管理机构、国家无线电监测中心应加强对干扰出现较多的频段和地区的日常无线电监测工作。

第十六条　涉及军地之间无线电干扰事宜，由国家无线电管理机构会同中国人民解放军电磁频谱管理机构通过军地协调机制协商解决。

第十七条　本办法自2017年9月1日起施行。

附件 1

无线电干扰投诉单

投诉单位（盖章）/投诉人：

<table>
<tr><td rowspan="3">基本信息</td><td>单位/姓名</td><td colspan="3"></td></tr>
<tr><td>通信地址</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>电　话</td><td></td></tr>
<tr><td colspan="2">受扰台站执照编号/频率使用许可文号</td><td></td><td>执照编号/频率许可有效期</td><td></td></tr>
<tr><td colspan="2">设台地址及经纬度</td><td colspan="3"></td></tr>
<tr><td colspan="2">受扰中心频率</td><td></td><td>带　宽</td><td></td></tr>
<tr><td colspan="2">极化方式</td><td></td><td>受扰起止时间</td><td></td></tr>
<tr><td colspan="2">疑似干扰源位置（选填）</td><td colspan="3"></td></tr>
<tr><td colspan="2">干扰自查情况</td><td colspan="3"></td></tr>
<tr><td>投诉内容摘要</td><td colspan="4">（可另附页）。
年　　月　　日

（可另附页）。

（可另附页）。</td></tr>
</table>

	（可另附页）。 （可另附页）。 （可另附页）。 （可另附页）。

附件 2

无线电干扰投诉排查任务回执单

基本信息	主办单位 （盖章）			任务单号		
	联系人			电　话		
	填表日期					
工作量统计	固定监测站（座）		移动监测站（座）		累计监测（小时）	
	派出人员 （人·天）			派出车辆（台次）		
干扰查处情况						

	（可另附页）

已采取措施	
下一步工作	

工业和信息化部关于印发《无线电干扰投诉和查处工作实施细则》的通知

（工信部无〔2018〕192号）

各省、自治区、直辖市无线电管理机构，国家无线电监测中心：

根据《中华人民共和国无线电管理条例》和《无线电干扰投诉和查处工作暂行办法》，制定《无线电干扰投诉和查处工作实施细则》。现予印发，请认真遵照执行。

工业和信息化部

2018年10月8日

无线电干扰投诉和查处工作实施细则

第一章　总则

第一条　为进一步规范无线电干扰查处工作流程，明确工作要求和任务分工，提高工作质量和效率，根据《中华人民共和国无线电管理条例》和《无线电干扰投诉和查处工作暂行办法》，结合工作实际，制定本细则。

第二条　国家无线电管理机构负责受理的境内外无线电干扰投诉的查处任务下达、执行、证据采集及归档等环节工作适用本细则（干扰查处流程图见附件1）。

第三条　根据无线电干扰所产生的危害程度和紧急程度，无线电干扰分为三个等级：第一级为危及国家安全、公共安全、生命财产安全以及影响重大活动正常用频的无线电干扰，第二级为严重影响党政机关、民用航空、广播电视和水上业务部门等重要用户依法开展无线电业务的无线电干扰，第三级为其他无线电干扰。

第二章　无线电干扰排查任务下达

第四条　国家无线电管理机构依据《无线电干扰投诉和查处工作暂行办法》受理、审查相关干扰投诉，根据无线电干扰等级，向国家无线电监测中心及各省、自治区、直辖市无线电管理机构下达无线电干扰投诉排查任务单。

第五条　对于第一级无线电干扰，国家无线电管理机构应在受理后立即下达无线电干扰排查任务；对于第二级无线电干扰，国家无线电管理机构应在受理后24小时内下达无线电干扰排查任务；对于第三级无线电干扰，国家无线电管理机构应在受理后48小时内下达无线电干扰排查任务。

第六条　各省、自治区、直辖市无线电管理机构以及国家无线电监测中心接到无线电干扰排查任务后，根据无线电干扰等级开展干扰排查工作。

对于第一级无线电干扰排查任务，应在接到任务后立即启动干扰监测，3天之内完成监测并报告结果；对于第二级无线电干扰排查任务，应在接到任务当日启动干扰监测，7天之内完成监测并报告结果；对于第三级无线电干扰排查任务，应在接到任务后24小时内启动干扰监测，10天之内完成监测并报告结果。

第三章　无线电干扰排查任务执行

第七条　国家无线电监测中心接到国家无线电管理机构下达的短波、卫星业务的无线电干扰监测和定位任务后，应根据所属监测站负责区域以及投诉的疑似干扰源位置确定牵头监测站，由牵头监测站组织实施干扰源的监测定位工作（国家无线电监测中心所属监测站负责区域见附件2）。

第八条　国家无线电监测中心应定期开展境外短波、卫星业务信号的监测工作，查找违反《无线电规则》、GE75协议和相关双边协议进行发射的境外信号，填写违章报告（《无线电规则》附录9）或有害干扰报告（《无线电规则》附录10），报国家无线电管理机构。

第九条　国家无线电监测中心在监测定位过程中发现的可能存在重大信息安全隐患的情况，应在第一时间通过电话等方式口头通知国家无线电管理机构，并在24小时内补交书面材料；国家无线电管理机构在收到口头通知后，应立即组织开展排查工作，及时消除信息安全隐患。

第十条　国家无线电监测中心应在无线电干扰投诉排查任务单规定时间内完成所有短波、卫星业务无线电干扰的监测定位工作，并将无线电干扰投诉排查任务回执单报国家无线电管理机构。对于未能在规定时间内完成定位的情况，需将具体原因及监测工作进展及时报国家无线电管理机构；对于干扰信号消失的情况，需向国家无线电管理机构申请监测延期，监测延期时限为7天。

国家无线电管理机构收到国家无线电监测中心无线电干扰投诉排查任务回执单后，应将定位结果告知投诉人并及时向干扰所在省、自治区、直辖市无线电管理机构下达干扰查处任务。

第十一条　各省、自治区、直辖市无线电管理机构接到国家无线电管理机构下达的无线电干扰查处任务后，应根据定位信息及时安排监测和执法人员开展干扰逼近查找和处置工作。发现涉及重大信息安全隐患的情况，应及时消除隐患并将有关情况报国家无线电管理机构。

第十二条　各省、自治区、直辖市无线电管理机构及其监测站应配备必要的覆盖短波、卫星频段的监测设备和干扰逼近查找设备。监测人员应具备短波、卫星干扰查找的基本技能。

第十三条　各省、自治区、直辖市无线电管理机构及其监测站应准确掌握区域内大功率短波发射台及卫星地球站的台站位置及工作频率，便于短波、卫星干扰查找工作的实施。

第十四条　各省、自治区、直辖市无线电管理机构及其监测站在逼近查找过程中，如需国家无线电监测中心进行短波、卫星干扰定位配合，可与国家无线电监测中心联系（联系方式见附件3）。

第十五条　各省、自治区、直辖市无线电管理机构及其监测站如因缺乏技术储备等原因，未能在规定的时间内完成短波及卫星业务无线电干扰排查任务，确需国家无线电监测中心派出人员以及设备协助进行干扰逼近查找，可向国家无线电监测中心发送协查函（见附件4），同时抄送国家无线电管理机构。国家无线电监测中心收到干扰协查函后，应立即安排所属监测站与相关无线电管理机构及其监测站取得联系并及时开展协查工作。

第十六条　各省、自治区、直辖市无线电管理机构及其监测站应在无线电干扰投诉排查任务单规定时间内完成查处工作，详细填写任务回执单并报国家无线电管理机构。对已查明的无线电干扰，任务回执单中查处情况应包含干扰源实际经纬度、频谱图、干扰源类别、干扰源所属单位或个人、干扰产生原因以及处置结果等要素；对未查明的无线电干扰，应在任务回执单中详细说明当前干扰排查情况以及下一步工作计划。

第四章　无线电干扰查处证据采集和归档

第十七条　用于监测数据采集的各类无线电监测设备应定期进行测试验证，确保监测

数据的准确性。用于监测数据采集的设备设置时间以及日期应与标准时间同步。

第十八条　在无线电干扰监测定位工作中，各省、自治区、直辖市无线电管理机构及其监测站和国家无线电监测中心应按照无线电干扰信号监测要求进行数据采集（无线电干扰信号监测要求见附件5）。

第十九条　各省、自治区、直辖市无线电管理机构及其监测站对干扰信号进行查处时，应加强对于书证、物证、视听资料、电子数据和证人证言以及当事人陈述等证据的规范采集记录以及保存。

第二十条　国家无线电管理机构应将无线电干扰投诉单、无线电干扰投诉排查任务单以及任务回执单等材料进行归档，并将当年干扰查处情况通报各相关单位；国家无线电监测中心应做好干扰监测、定位报告的归档分析工作；各省、自治区、直辖市无线电管理机构及其监测站应做好干扰查处相关证据、资料的归档整理工作。

第二十一条　本规定自印发之日起施行。

附件：1. 干扰查处流程图

2. 国家无线电中心所属监测站负责区域

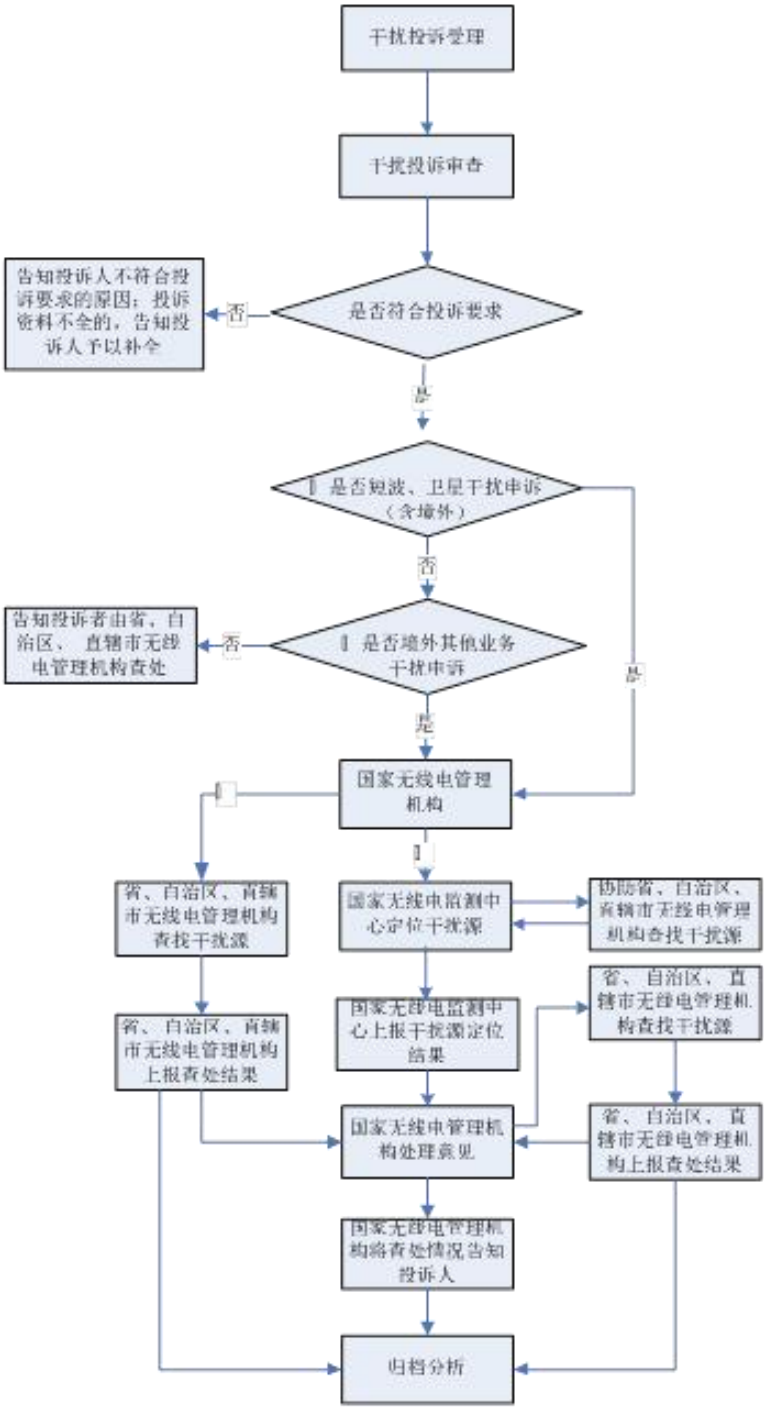
3. 联系方式

4. 无线电干扰协查函模板

5. 无线电干扰信号监测要求

附件 1

干扰查处流程图



附件 2

国家无线电监测中心所属监测站负责区域

国家无线电监测中心所属监测站	短波负责区域
北京站	北京 天津 河北 山东
哈尔滨站	辽宁 内蒙古 吉林 黑龙江
上海站	上海 浙江 江苏
福建站	福建 江西 湖南
深圳站	广东 广西 海南
云南站	云南 贵州
成都站	四川 重庆 西藏
陕西站	陕西 河南 湖北 山西
乌鲁木齐站	新疆 宁夏 甘肃 青海

国家无线电监测中心所属监测站	卫星负责区域
北京站	长江以北省份
深圳站	长江以南省份

附件 3

联系方式

工业和信息化部无线电管理局

监督检查处：010-68206252

国家无线电监测中心

无线电监测处：010-68009120（短波业务干扰定位）

010-68009121（卫星业务干扰定位）

附件 4

XX 省（自治区、直辖市）无线电管理机构关于商请协助完成无线电干扰逼近查找工作的函

国家无线电监测中心：

按照工业和信息化部无线电管理局关于XXX工作（第20XXXX号任务）要求，因XXX（原因），为及时完成此项工作，我X拟请你中心于XXXX年XX月XX日派出监测组赴XX省XX市协助开展干扰逼近查找工作。

请予配合为盼。

XX省（自治区、直辖市）无线电管理机构

201X年XX月XX日

（联系人及电话：XX，XXXX-XXXXXXXX）

抄送：工业和信息化部无线电管理局

附件5

无线电干扰信号监测要求

一、无线电干扰信号监测的技术参数，包括频率、带宽、电平或场强、调制类型、极化方式（卫星）和轨道位置（卫星）等，并保存必要的频谱信息软件截图，以判断其是否对合法用户造成干扰。

二、如进行无线电测向定位或卫星干扰源定位，应保存定位信息截图。

三、如进行移动监测车逼近查找，应记录查找路径、测试地点的位置坐标，并保存场强变化明显区域的频谱图。（位置坐标均采用WGS-84坐标系）

四、利用频谱仪或监测接收机接收干扰信号并保存频谱图时，应将监测设备中心频率设置为干扰信号的频率，监测频段跨宽（Span）大于干扰信号占用带宽的1.5-2倍，频谱仪分辨率带宽（RBW）或监测接收机中频带宽小于1/50干扰信号占用带宽，并确保监测设备显示干扰信号的最大电平值或场强值，使干扰信号区别于底噪清晰显示于频谱图中。

五、到达干扰信号发射区域，应记录干扰信号近场发射频谱图，将监测设备显示频谱图与发射天线或周边环境位置标记同框拍照，记录该地点的位置坐标。如对发射设备进行开关机测试，应保存设备开机与关机后的频谱图及现场工作照片，并记录现场的位置坐标。

工业和信息化部办公厅印发《关于推进综合整治骚扰电话专项行动的工作方案》的通知

（工信厅信管函〔2018〕337号）

各省、自治区、直辖市通信管理局，中国信息通信研究院，中国互联网协会、中国通信标准化协会，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，各相关企业：

为落实工业和信息化部等13部门《综合整治骚扰电话专项行动方案》（工信部联信管〔2018〕138号）有关要求，加强通信渠道管控，提升技术防范能力，全面遏制骚扰电话蔓延，现将《关于推进综合整治骚扰电话专项行动的工作方案》印发你们，请结合工作实际，认真贯彻执行。

工业和信息化部办公厅

2018年10月27日

关于推进综合整治骚扰电话专项行动的工作方案

为贯彻落实工业和信息化部等13部门《综合整治骚扰电话专项行动方案》（工信部联信管〔2018〕138号），推进骚扰电话治理工作，净化通信服务环境，保障用户合法权益，特制定本方案。

一、工作目标

全面加强通信资源管理，完善骚扰电话的发现、举报、处置流程，切断骚扰电话传播渠道；加强技术手段建设，提升骚扰电话防范能力；综合调动各方力量，规范电话营销行为，建立骚扰电话长效管控机制，实现商业营销类电话规范拨打、恶意骚扰和违法犯罪类电话明显减少的目标，营造良好的通信环境。

二、工作任务

（一）加强通信资源和用户管理

各基础电信企业要按照“谁接入谁负责”的原则，加强业务管理，强化用户约束，防范各类通信资源被用于电话扰民。

1.全面核查清理。全面清查语音专线、“95”“96”“400”号码等资源使用情况，重点清查金融保险、地产中介、零售推销等行业及呼叫中心企业的专线和码号使用情况。严禁擅自改变码号资源用途，严禁为经营性呼叫中心的外呼业务核配用户号码，严禁为非法经营、超范围经营电信业务的企业提供通信资源，不符合资源使用规范的专线一律关停。（2018年11月底前）

2.严格台账管理。建立语音专线、“95”“96”“400”号码等资源的台账，汇总至集团公司并报属地通信管理局，包括使用主体、接入信息、用户资质、资源用途等信息。建立动态巡查更新机制，确保相关台账信息真实准确，电信管理机构可依法随时查询溯源。（2018年12月底前）

3.加强新用户管理。严格审查新用户资质，申请用户应当提供有效证照，经营电信业务的，必须提供相应的电信业务经营许可证。严格核实资源使用用途，督促企业客户不得将办公自用电信资源用于经营电信业务。在提供通信资源和进行业务合作时，要将电信业务经营不良名单和失信名单作为重要考量因素。

4.加强电话用户合同约束。各基础电信企业、移动转售企业要全面完善个人用户和集团用户合同管理，在合同中明确约定通信资源和业务使用规范要求、用户违约责任，增加骚扰电话拦截和处置相关条款，明确呼叫频次限制和骚扰电话举报处置措施，并逐步替换存量合同或签署补充条款。（2019年10月底前）

（二）全面规范呼叫中心业务

各呼叫中心企业要严格落实企业主体责任，规范自身外呼行为，完善商业营销外呼管理机制，不得营销扰民。

1.规范通信资源使用行为。全面梳理自身业务，经营性呼叫中心不得使用用户号码作为业务号码，不得超范围经营；对存量资源进行全面自查整改，不得非法转租转售通信资源。（2019年3月底前）

2.规范营销外呼行为。开展商业性营销，应事先征得用户同意，保留相关凭证并积极配合骚扰电话核查工作。除即时回访类业务外，主动外呼行为须避开用户的日常休息时段，不得按号段盲呼。

3.建立禁呼名单制度。全面建立禁呼名单制度，用户明确表示拒绝特定行业或业务的营销电话后，不得再次拨打。确需通过外呼方式为用户提供服务的，要严格控制外呼时间

和频次，并在一定时段内（原则上不少于30日）留存通话录音。（2018年12月底前）

（三）全面清理各类骚扰软件

各相关互联网企业（含信息发布平台、电商平台、应用软件分发平台和社交平台）要全面清理“呼死你”“网络改号”“短信轰炸机”等软件及“猫池”“语音网关”等设备相关销售推广信息，切断相关软件、设备在互联网上的搜索、发布、下载、交易渠道。建立动态查处清理机制，让相关软件和设备信息“发不出、搜不到、用不了”，发现一起清除一起。（2018年11月底前）

（四）提升技术防范能力

1.强化主叫号码鉴权和溯源能力

各基础电信企业要落实主叫鉴权要求，对未通过鉴权的呼叫一律进行拦截。禁止客户自行修改主叫号码，严禁利用透传技术虚拟主叫号码。要全面建立骚扰电话内部核查处理问责机制，集团及省公司均设立专人负责。留存30日的信令数据，做好骚扰电话溯源核查工作，并为相关移动转售企业提供必要的支持。（2018年11月底前）

2.提升骚扰电话监测和拦截能力

（1）各基础电信企业要建立和完善骚扰电话拦截系统，运用大数据等技术手段，充分结合信令监测、呼叫行为分析，建立骚扰电话拦截策略，完善骚扰电话拦截流程。严格落实相关技术标准和规范要求，加强“＋86”国际虚假主叫拦截，做好虚假主叫、不规范主叫、“响一声”、“呼死你”等骚扰电话的甄别和拦截工作。（2019年6月底前）

（2）各通信管理局要充分利用现有全国诈骗电话防范系统和网间互联互通监测系统，做好骚扰电话数据的收集和分析工作，提升骚扰电话监测发现能力，强化对录音类骚扰电话和已发现骚扰电话的拦截能力，并做好与基础电信企业的联动工作。

3.加强骚扰电话风险提示能力

（1）中国通信标准化协会要加快制定移动智能终端防骚扰技术要求、骚扰标记分类等骚扰电话治理相关标准，规范标记行为。

（2）鼓励各智能终端制造企业在手机终端引入骚扰电话防范功能，为用户提供快捷方便的骚扰电话识别、处置功能。鼓励各互联网企业开发具备骚扰电话标注、拦截和风险防控警示功能的应用软件。

（3）各基础电信企业、移动转售企业要完善相关技术手段，具备通过短信、闪信等业

务为国内手机用户提供涉嫌骚扰电话来电号码标注提醒和风险防控警示能力。（2019 年 3 月底前）

（4）中国信息通信研究院要建立高危号码标记、核查、处理、更新更正机制，及时向社会公开标记信息，全面提高码号标记准确性。初步建成全国防骚扰信息综合服务平台，汇总用户对各类营销电话的接收意愿并与基础电信企业、移动转售企业和呼叫中心企业等共享数据。各相关企业应根据用户意愿有效拦截特定行业或业务的营销电话。（2019 年 12 月底前）

（5）各基础电信企业、呼叫中心企业及互联网企业要加强与各单位合作，提供必要的技术和资源协助，共同建立健全骚扰电话防范体系。

（五）建立健全骚扰电话管控机制

1.畅通骚扰电话投诉举报渠道。工业和信息化部委托中国互联网协会 12321 网络不良和垃圾信息举报中心统一受理骚扰电话举报，并实时将相关举报情况通报各通信管理局、基础电信企业和移动转售企业。中国信息通信研究院、中国互联网协会要推动基础电信企业全面建成网间投诉联动协查机制。（2018 年 12 月底前）

2.完善骚扰电话举报处置机制。各基础电信企业、移动转售企业要建立骚扰电话举报处置机制，及时核实处置用户举报并向被举报人反馈。对因处置骚扰电话产生用户申诉的，核实相关骚扰电话举报属实的，可在用户申诉考核中予以核减。（2019 年 3 月底前）

3.加强骚扰电话问题责任追究。各通信管理局要引导企业强化骚扰电话治理意识，严格落实骚扰电话治理相关要求。对骚扰电话举报投诉、违法违规问题、媒体曝光造成恶劣影响的事件要追根溯源，有案必查，查实必罚。对问题严重的主要负责人和具体责任人，要严肃处理。

4.强化信用管理。对因骚扰电话问题受到行政处罚的企业，各通信管理局要及时将其纳入电信业务经营不良名单，并向社会公布。各基础电信企业要建立合作伙伴和客户信用管理机制，对骚扰电话、垃圾信息突出的客户进行必要的提醒和警示，并建立企业间相关信息共享机制。

5.建立部门沟通协作机制。各通信管理局要结合自身实际工作情况，建立与本地区各行业管理部门的沟通协调机制，推动骚扰电话源头治理。（2018 年 11 月底前）

（六）强化行业自律

各基础电信企业、移动转售企业和互联网企业要规范自身电话业务营销行为。鼓励行业协会等加强行业自律体系建设，联合基础电信企业、移动转售企业、呼叫中心企业，推动话音业务规范、技术手段防控、关键数据共享、营销业务服务规范，出台营销电话规范等自律公约。

三、工作要求

（一）强化考核监督。各基础电信企业应将骚扰电话整治工作纳入基层单位关键绩效考核。各通信管理局要强化监督检查，依法查处各类违规行为。工业和信息化部适时组织抽查并通报相关情况。

（二）加强宣传引导。各单位要切实加强社会宣传工作，曝光违法违规企业和典型案例，及时答复和响应人民群众反映的问题和诉求，适时回应社会关注的热点问题，主动接受社会舆论监督。

（三）定期通报总结。各单位要加强工作检查和信息通报，分析总结治理工作经验，探索建立骚扰电话管控的长效机制。2018 年第四季度开始，各通信管理局、基础电信企业要按季度将治理工作情况总结报工业和信息化部（信息通信管理局）。

互联网信息服务管理办法

（2000 年 9 月 25 日中华人民共和国国务院令第 292 号公布　根据 2011 年 1 月 8 日《国务院关于废止和修改部分行政法规的决定》修订）

第一条　为了规范互联网信息服务活动，促进互联网信息服务健康有序发展，制定本办法。

第二条　在中华人民共和国境内从事互联网信息服务活动，必须遵守本办法。

本办法所称互联网信息服务，是指通过互联网向上网用户提供信息的服务活动。

第三条　互联网信息服务分为经营性和非经营性两类。

经营性互联网信息服务，是指通过互联网向上网用户有偿提供信息或者网页制作等服务活动。

非经营性互联网信息服务，是指通过互联网向上网用户无偿提供具有公开性、共享性信息的服务活动。

第四条　国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度。

未取得许可或者未履行备案手续的，不得从事互联网信息服务。

第五条　从事新闻、出版、教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。

第六条　从事经营性互联网信息服务，除应当符合《中华人民共和国电信条例》规定的要求外，还应当具备下列条件：

（一）有业务发展计划及相关技术方案；

（二）有健全的网络与信息安全保障措施，包括网站安全保障措施、信息安全保密管理制度、用户信息安全管理制度；

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门同意的文件。

第七条　从事经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门申请办理互联网信息服务增值电信业务经营许可证（以下简称经

营许可证）。

省、自治区、直辖市电信管理机构或者国务院信息产业主管部门应当自收到申请之日起60日内审查完毕，作出批准或者不予批准的决定。予以批准的，颁发经营许可证；不予批准的，应当书面通知申请人并说明理由。

申请人取得经营许可证后，应当持经营许可证向企业登记机关办理登记手续。

第八条 从事非经营性互联网信息服务，应当向省、自治区、直辖市电信管理机构或者国务院信息产业主管部门办理备案手续。办理备案时，应当提交下列材料：

（一）主办单位和网站负责人的基本情况；

（二）网站网址和服务项目；

（三）服务项目属于本办法第五条规定范围的，已取得有关主管部门的同意文件。

省、自治区、直辖市电信管理机构对备案材料齐全的，应当予以备案并编号。

第九条 从事互联网信息服务，拟开办电子公告服务的，应当在申请经营性互联网信息服务许可或者办理非经营性互联网信息服务备案时，按照国家有关规定提出专项申请或者专项备案。

第十条 省、自治区、直辖市电信管理机构和国务院信息产业主管部门应当公布取得经营许可证或者已履行备案手续的互联网信息服务提供者名单。

第十一条 互联网信息服务提供者应当按照经许可或者备案的项目提供服务，不得超出经许可或者备案的项目提供服务。

非经营性互联网信息服务提供者不得从事有偿服务。

互联网信息服务提供者变更服务项目、网站网址等事项的，应当提前30日向原审核、发证或者备案机关办理变更手续。

第十二条 互联网信息服务提供者应当在其网站主页的显著位置标明其经营许可证编号或者备案编号。

第十三条 互联网信息服务提供者应当向上网用户提供良好的服务，并保证所提供的信息内容合法。

第十四条 从事新闻、出版以及电子公告等服务项目的互联网信息服务提供者，应当记录提供的信息内容及其发布时间、互联网地址或者域名；互联网接入服务提供者应当记录上网用户的上网时间、用户账号、互联网地址或者域名、主叫电话号码等信息。

互联网信息服务提供者和互联网接入服务提供者的记录备份应当保存60日，并在国家有关机关依法查询时，予以提供。

第十五条 互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第十六条 互联网信息服务提供者发现其网站传输的信息明显属于本办法第十五条所列内容之一的，应当立即停止传输，保存有关记录，并向国家有关机关报告。

第十七条 经营性互联网信息服务提供者申请在境内境外上市或者同外商合资、合作，应当事先经国务院信息产业主管部门审查同意；其中，外商投资的比例应当符合有关法律、行政法规的规定。

第十八条 国务院信息产业主管部门和省、自治区、直辖市电信管理机构，依法对互联网信息服务实施监督管理。

新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理。

第十九条 违反本办法的规定，未取得经营许可证，擅自从事经营性互联网信息服务，或者超出许可的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正，有违法所得的，没收违法所得，处违法所得3倍以上5倍以下的罚款；没有违法所得或者违法所得不足5万元的，处10万元以上100万元以下的罚款；情节严重的，责令关闭网站。

违反本办法的规定，未履行备案手续，擅自从事非经营性互联网信息服务，或者超出备案的项目提供服务的，由省、自治区、直辖市电信管理机构责令限期改正；拒不改正的，责令关闭网站。

第二十条 制作、复制、发布、传播本办法第十五条所列内容之一的信息，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由公安机关、国家安全机关依照《中华人民共和国治安管理处罚法》、《计算机信息网络国际联网安全保护管理办法》等有关法律、行政法规的规定予以处罚；对经营性互联网信息服务提供者，并由发证机关责令停业整顿直至吊销经营许可证，通知企业登记机关；对非经营性互联网信息服务提供者，并由备案机关责令暂时关闭网站直至关闭网站。

第二十一条 未履行本办法第十四条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，责令停业整顿或者暂时关闭网站。

第二十二条 违反本办法的规定，未在其网站主页上标明其经营许可证编号或者备案编号的，由省、自治区、直辖市电信管理机构责令改正，处5000元以上5万元以下的罚款。

第二十三条 违反本办法第十六条规定的义务的，由省、自治区、直辖市电信管理机构责令改正；情节严重的，对经营性互联网信息服务提供者，并由发证机关吊销经营许可证，对非经营性互联网信息服务提供者，并由备案机关责令关闭网站。

第二十四条 互联网信息服务提供者在其业务活动中，违反其他法律、法规的，由新闻、出版、教育、卫生、药品监督管理和工商行政管理等有关主管部门依照有关法律、法规的规定处罚。

第二十五条 电信管理机构和其他有关主管部门及其工作人员，玩忽职守、滥用职权、徇私舞弊，疏于对互联网信息服务的监督管理，造成严重后果，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，对直接负责的主管人员和其他直接责任人员依法给予降级、撤职直至开除的行政处分。

第二十六条 在本办法公布前从事互联网信息服务的，应当自本办法公布之日起60日内依照本办法的有关规定补办有关手续。

第二十七条 本办法自公布之日起施行。

互联网信息内容管理行政执法程序规定

国家互联网信息办公室令

第 2 号

《互联网信息内容管理行政执法程序规定》已经国家互联网信息办公室室务会议审议通过,现予公布,自 2017 年 6 月 1 日起施行。

主任 徐麟

2017 年 5 月 2 日

第一章 总则

第一条 为了规范和保障互联网信息内容管理部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国行政处罚法》、《中华人民共和国网络安全法》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 互联网信息内容管理部门依法实施行政执法,对违反有关互联网信息内容管理法律法规规章的行为实施行政处罚，适用本规定。

本规定所称互联网信息内容管理部门，是指国家互联网信息办公室和地方互联网信息办公室。

第三条 互联网信息内容管理部门实施行政执法，应当遵循公开、公平、公正的原则，做到事实清楚、证据确凿、程序合法、法律法规规章适用准确适当、执法文书使用规范。

第四条 互联网信息内容管理部门建立行政执法督查制度。

上级互联网信息内容管理部门对下级互联网信息内容管理部门实施的行政执法进行督查。

第五条 互联网信息内容管理部门应当加强执法队伍建设，建立健全执法人员培训、考试考核、资格管理和持证上岗制度。

执法人员应当参加互联网信息内容管理部门组织的法律知识和业务知识培训，并经行政执法资格考试或者考核合格，取得执法证后方可从事执法工作。

执法证由国家互联网信息内容管理部门统一制定、核发或者授权省、自治区、直辖市

互联网信息内容管理部门核发。

第二章 管辖

第六条 行政处罚由违法行为发生地的互联网信息内容管理部门管辖。

违法行为发生地包括实施违法行为的网站备案地，工商登记地（工商登记地与主营业地不一致的，应按主营业地），网站建立者、管理者、使用者所在地，网络接入地，计算机等终端设备所在地等。

第七条 市（地、州）级以下互联网信息内容管理部门依职权管辖本行政区域内的互联网信息内容行政处罚案件。

省、自治区、直辖市互联网信息内容管理部门依职权管辖本行政区域内重大、复杂的互联网信息内容行政处罚案件。

国家互联网信息内容管理部门依职权管辖应当由自己实施行政处罚的案件及全国范围内发生的重大、复杂的互联网信息内容行政处罚案件。

省、自治区、直辖市互联网信息内容管理部门可以依据法律法规规章，结合本地区实际，制定本行政区域内级别管辖的具体规定。

第八条 对当事人的同一违法行为，两个以上互联网信息内容管理部门均有管辖权的，由先行立案的互联网信息内容管理部门管辖。必要时，可以移送主要违法行为发生地的互联网信息内容管理部门管辖。

两个以上的互联网信息内容管理部门对管辖权有争议的，应当协商解决；协商不成的，报请共同的上一级互联网信息内容管理部门指定管辖。

第九条 上级互联网信息内容管理部门认为必要时，可以直接办理下级互联网信息内容管理部门管辖的案件，也可以将自己管辖的案件移交下级互联网信息内容管理部门办理。

下级互联网信息内容管理部门对其管辖的案件由于特殊原因不能行使管辖权的，可以报请上级互联网信息内容管理部门管辖或者指定管辖。

第十条 互联网信息内容管理部门发现案件不属于其管辖的，应当及时移送有管辖权的互联网信息内容管理部门。

受移送的互联网信息内容管理部门应当将案件查处结果及时函告移送案件的互联网信息内容管理部门；认为移送不当的，应当报请共同的上一级互联网信息内容管理部门指定管辖，不得再次移送。

第十一条 上级互联网信息内容管理部门接到管辖争议或者报请指定管辖请示后,应当在十个工作日内作出指定管辖的决定，并书面通知下级互联网信息内容管理部门。

第十二条 互联网信息内容管理部门发现案件属于其他行政机关管辖的,应当依法移送有关机关。

互联网信息内容管理部门发现违法行为涉嫌犯罪的，应当及时移送司法机关。司法机关决定立案的，互联网信息内容管理部门应当自接到司法机关立案通知书之日起三日内将与案件有关的材料移交司法机关，并办结交接手续。

第十三条 互联网信息内容管理部门对依法应当撤销互联网新闻信息服务许可、吊销互联网新闻信息服务许可证的，应当提出处理建议，并将取得的证据及相关材料报送原发证的互联网信息内容管理部门,由原发证的互联网信息内容管理部门依法作出是否撤销许可、吊销许可证的决定。

第三章 立案

第十四条 互联网信息内容管理部门应当对下列事项及时调查处理，并填写《案件来源登记表》：

（一）在监督检查中发现案件线索的；

（二）自然人、法人或者其他组织投诉、申诉、举报的；

（三）上级机关交办或者下级机关报请查处的；

（四）有关部门移送或者经由其他方式、途径披露的。

第十五条 行政处罚立案应当符合下列条件：

（一）有涉嫌违法的事实；

（二）依法应当予以行政处罚的；

（三）属于互联网信息内容监督管理行政处罚的范围；

（四）属于本互联网信息内容管理部门管辖。

符合立案条件的，应当填写《立案审批表》，同时附上相关材料，在七个工作日内报互联网信息内容管理部门负责人批准立案，并确定两名以上执法人员为案件承办人。特殊情况下，可以延长至十五个工作日内立案。

第十六条 对于不予立案的投诉、申诉、举报，经互联网信息内容管理部门负责人批准后，应将结果告知具名的投诉人、申诉人、举报人，并将不予立案的相关情况作书面记录

留存。

对于其他部门移送的案件，决定不予立案的，应当书面告知移送部门。

不予立案或者撤销立案的，承办人应当制作《不予立案审批表》或者《撤销立案审批表》，报互联网信息内容管理部门负责人批准。

第十七条 办案人员有下列情形之一的，应当自行回避；当事人也有权申请办案人员回避：

（一）是本案的当事人或者当事人的近亲属；

（二）与本案有直接利害关系；

（三）与本案当事人有其他关系，可能影响案件公正处理的。

办案人员的回避由互联网信息内容管理部门负责人决定。当事人对决定不服的，可以申请复议一次。

回避决定作出前，被申请回避人员不停止对案件的调查处理。

第四章 调查取证

第十八条 互联网信息内容管理部门进行案件调查取证时，执法人员不得少于两人，并应当出示执法证。必要时，也可以聘请专业人员进行协助。

首次向案件当事人收集、调取证据的，应当告知其有申请办案人员回避的权利。

向有关单位、个人收集、调取证据时，应当告知其有如实提供证据的义务。被调查对象或者有关人员应当如实回答询问并协助、配合调查，及时提供依法应当保存的互联网信息服务提供者发布的信息、用户发布的信息、日志信息等相关材料，不得阻挠、干扰案件的调查。

执法人员对在办案过程中知悉的国家秘密、商业秘密、个人隐私、个人信息应当依法保密。

第十九条 互联网信息内容管理部门在办案过程中需要其他地区互联网信息内容管理部门协助调查、取证的，应当出具委托调查函。受委托的互联网信息内容管理部门应当积极予以协助，一般应当在接到委托调查函之日起十五个工作日内完成相关工作；需要延期完成或者无法协助的，应当及时函告委托互联网信息内容管理部门。

第二十条 办案人员应当依法收集与案件有关的证据，包括电子数据、视听资料、书证、物证、证人证言、当事人的陈述、鉴定意见、检验报告、勘验笔录、现场笔录、询问笔录

等。

电子数据是指案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的一切数据，包括但不限于网页、博客、微博客、即时通信工具、论坛、贴吧、网盘、电子邮件、网络后台等方式承载的电子信息或文件。电子数据主要存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或存储介质中。视听资料包括录音资料和影像资料。

存储在电子介质中的录音资料和影像资料，适用电子数据的规定。

第二十一条 互联网信息内容管理部门在立案前调查或者检查过程中依法取得的证据，可以作为认定事实的依据。通过网络巡查等技术手段获取的、具有可靠性的电子数据可以作为认定事实的依据。

电子数据的收集、提取应当符合法律法规规章、国家标准、行业标准和技术规范，并保证所收集、提取的电子数据的完整性、合法性、真实性、关联性。否则，不得作为认定事实的依据。

第二十二条 互联网信息内容管理部门在立案前，可以采取询问、勘验、检查、鉴定、调取证据材料等措施，不得限制初查对象的人身、财产权利。

互联网信息内容管理部门在立案后，可以对物品、设施、场所采取先行登记保存等措施。

第二十三条 互联网信息内容管理部门在办案过程中，应当及时询问证人。

执法人员进行询问的，应当制作《询问笔录》，载明时间、地点、有关事实、经过等内容。询问笔录应当交询问对象或者有关人员核对并确认。

第二十四条 互联网信息内容管理部门对于涉及互联网信息内容违法的场所、物品、网络应当进行勘验、检查，及时收集、固定书证、物证、视听资料以及电子数据。

第二十五条 互联网信息内容管理部门可以委托司法鉴定机构就案件中的专门性问题出具鉴定意见；不属于司法鉴定范围的，可以委托有能力或者条件的机构出具检测报告或者检验报告。

第二十六条 互联网信息内容管理部门可以向有关单位、个人调取能够证明案件事实的证据材料，并且可以根据需要拍照、录像、复印和复制。

调取的书证、物证应当是原件、原物。调取原件、原物确有困难的，可以由提交证据

的有关单位、个人在复制品上签字或者盖章，注明“此件由×××提供，经核对与原件（物）无异”的字样或者文字说明，并注明出证日期、证据出处，并签名或者盖章。

调取的视听资料、电子数据应当是原始载体或备份介质。调取原始载体或备份介质确有困难的，可以收集复制件，并注明制作方法、制作时间、制作人等情况。调取声音资料的应当附有该声音内容的文字记录。

第二十七条 在证据可能灭失或者以后难以取得的情况下，经互联网信息内容管理部门负责人批准，执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存，制作《登记保存物品清单》，向当事人出具《登记保存物品通知书》。先行登记保存期间，当事人或有关人员不得损毁、销毁或者非法转移证据。

互联网信息内容管理部门实施先行登记保存时，应当通知当事人或者持有人到场，并在现场笔录中对采取的相关措施情况予以记载。

第二十八条 互联网信息内容管理部门对先行登记保存的证据，应当在七日内作出以下处理决定：

（一）需要采取证据保全措施的，采取记录、复制、拍照、录像等证据保全措施后予以返还；

（二）需要检验、检测、鉴定的，送交具有相应资质的机构检验、检测、鉴定；

（三）违法事实成立的，依法应当予以没收的，作出行

政处罚决定，没收违法物品；

（四）违法事实不成立，或者违法事实成立但依法不应当予以没收的，解除先行登记保存。

逾期未作出处理决定的，应当解除先行登记保存。

第二十九条 为了收集、保全电子数据，互联网信息内容管理部门可以采取现场取证，远程取证，责令有关单位、个人固定和提交等措施。

现场取证、远程取证结束后应当制作《电子取证工作记录》。

第三十条 执法人员在调查取证过程中，应当要求当事人在笔录或者其他材料上签字、捺指印、盖章或者以其他方式确认。当事人拒绝到场，拒绝签字、捺指印、盖章或者以其他方式确认，或者无法找到当事人的，应当由两名执法人员在笔录或者其他材料上注明原

因，并邀请有关人员作为见证人签字或者盖章，也可以采取录音、录像等方式记录。

第三十一条 案件调查终结后，承办人应当撰写《案件处理意见报告》：

认为违法事实成立，应当予以行政处罚的，撰写《案件处理意见报告》，草拟行政处罚建议书。

有下列情形之一的，撰写《案件处理意见报告》，说明拟作处理的理由，报互联网信息内容管理部门负责人批准后根据不同情况分别处理：

（一）认为违法事实不成立，应当予以销案的；

（二）违法行为情节轻微，没有造成危害后果，不予行政处罚的；

（三）案件不属于本机关管辖，应当移送其他行政机关管辖的；

（四）涉嫌犯罪，应当移送司法机关的。

第三十二条 互联网信息内容管理部门进行案件调查时,对已有证据证明违法事实成立的，应当出具责令改正通知书，责令当事人改正或者限期改正违法行为。

第五章 听证、约谈

第三十三条 互联网信息内容管理部门作出吊销互联网新闻信息服务许可证、较大数额罚款等行政处罚决定之前，应当告知当事人有要求举行听证的权利。当事人要求听证的，应当在被告知后三日内提出，互联网信息内容管理部门应当组织听证。当事人逾期未要求听证的，视为放弃权利。

第三十四条 互联网信息内容管理部门应当在听证的七日前，将《举行听证通知书》送达当事人，告知举行听证的时间、地点。

听证应当制作《听证笔录》，交当事人审核无误后签字或者盖章。

第三十五条 互联网信息内容管理部门对互联网信息服务提供者违法行为作出行政处罚决定前，可以根据有关规定对其实施约谈，谈话结束后制作《执法约谈笔录》。

第六章 处罚决定、送达

第三十六条 互联网信息内容管理部门作出行政处罚决定之前，应当填写《行政处罚意见告知书》，告知当事人拟作出行政处罚的违法事实、处罚的理由和依据，以及当事人依法享有的陈述、申辩权。

互联网信息内容管理部门应当充分听取当事人的陈述和申辩。当事人提出的事实、理由或者证据经复核成立的，应当采纳。当事人在接到告知书之日起三个工作日内未提出陈

述、申辩的，视为放弃权利。

互联网信息内容管理部门不得因当事人陈述、申辩而加重处罚。

第三十七条 拟作出的行政处罚决定应当报互联网信息内容管理部门负责人审查。互联网信息内容管理部门负责人根据不同情况，分别作出如下决定：

（一）确有应受行政处罚的违法行为的，根据情节轻重及具体情况，作出行政处罚决定；

（二）违法行为轻微，依法可以不予行政处罚的，不予行政处罚；

（三）违法事实不能成立的，不予行政处罚；

（四）违法行为已构成犯罪的，移送司法机关。

第三十八条 对情节复杂或者重大违法行为给予较重的行政处罚，互联网信息内容管理部门负责人应当集体讨论决定。集体讨论决定的过程应当有书面记录。

情节复杂、重大违法行为标准由互联网信息内容管理部门根据实际情况确定。

第三十九条 互联网信息内容管理部门作出行政处罚决定，应当制作统一编号的《行政处罚决定书》。

《行政处罚决定书》应当载明下列事项：

（一）当事人的姓名或者名称、地址等基本情况；

（二）违反法律、法规或者规章的事实和证据；

（三）行政处罚的种类和依据；

（四）行政处罚的履行方式和期限；

（五）不服行政处罚决定，申请行政复议或者提起行政诉讼的途径和期限；

（六）作出行政处罚决定的互联网信息内容管理部门名称和作出决定的日期。

行政处罚决定中涉及没收有关物品的，还应当附没收物品凭证。

《行政处罚决定书》应当盖有作出行政处罚决定的互联网信息内容管理部门的印章。

第四十条 《行政处罚决定书》应当在宣告后当场交付当事人；当事人不在场的，应当在七日内依照民事诉讼法的有关规定，将《行政处罚决定书》送达当事人。

第七章 执行与结案

第四十一条 《行政处罚决定书》送达后，当事人应当在处罚决定的期限内予以履行。

当事人确有经济困难，可以提出延期或者分期缴纳罚款的申请，并提交书面材料。经

案件承办人审核，确定延期或者分期缴纳罚款的期限和金额，报互联网信息内容管理部门负责人批准后执行。

第四十二条 互联网信息服务提供者违反相关法律法规规章,需由电信主管部门关闭网站、吊销互联网信息服务增值电信业务经营许可证或者取消备案的，转电信主管部门处理。

第四十三条 当事人对互联网信息内容管理部门给予的行政处罚享有陈述、申辩权，对行政处罚决定不服的，有权依法申请行政复议或者提起行政诉讼。

当事人对行政处罚决定不服，申请行政复议或者提起行政诉讼的，行政处罚不停止执行，法律另有规定的除外。

第四十四条 当事人在法定期限内不申请行政复议或者提起行政诉讼,又不履行行政处罚决定的，作出处罚决定的互联网信息内容管理部门可以申请人民法院强制执行。

互联网信息内容管理部门申请人民法院强制执行前应当填写《履行行政处罚决定催告书》，书面催告当事人履行义务，并告知履行义务的期限和方式、依法享有的陈述和申辩权，涉及加处罚款的，应当有明确的金额和给付方式。

加处罚款的总数额不得超过原罚款数额。

当事人进行陈述、申辩的，互联网信息内容管理部门应当对当事人提出的事实、理由和证据进行记录、复核，并制作陈述申辩笔录、陈述申辩复核意见书。当事人提出的事实、理由或者证据成立的，互联网信息内容管理部门应当采纳。

《履行行政处罚决定催告书》送达十个工作日后，当事人仍未履行处罚决定的，互联网信息内容管理部门可以申请人民法院强制执行，并填写《行政处罚强制执行申请书》。

第四十五条 行政处罚决定履行或者执行后，办案人应当填写《行政处罚结案报告》，将有关案件材料进行整理装订，归档保存。

第八章 附则

第四十六条 本规定中的期限以时、日计算，开始的时和日不计算在内。期限届满的最后一日是节假日的，以节假日后的第一日为届满的日期。法律、法规另有规定的除外。

第四十七条 本规定中的“以上”、“以下”、“以内”，均包括本数。

第四十八条 国家互联网信息内容管理部门负责制定行政执法所适用的文书格式范本。各省、自治区、直辖市互联网信息内容管理部门可以参照文书格式范本，制定本行政区域行政处罚所适用的文书格式并自行印制。

第四十九条 本规定自2017年6月1日起施行。

互联网新闻信息服务管理规定

国家互联网信息办公室令

第 1 号

《互联网新闻信息服务管理规定》已经国家互联网信息办公室室务会议审议通过，现予公布，自 2017 年 6 月 1 日起施行。

主任 徐麟

2017 年 5 月 2 日

互联网新闻信息服务管理规定

第一章 总则

第一条 为加强互联网信息内容管理，促进互联网新闻信息服务健康有序发展，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 在中华人民共和国境内提供互联网新闻信息服务，适用本规定。

本规定所称新闻信息，包括有关政治、经济、军事、外交等社会公共事务的报道、评论，以及有关社会突发事件的报道、评论。

第三条 提供互联网新闻信息服务，应当遵守宪法、法律和行政法规，坚持为人民服务、为社会主义服务的方向，坚持正确舆论导向，发挥舆论监督作用，促进形成积极健康、向上向善的网络文化，维护国家利益和公共利益。

第四条 国家互联网信息办公室负责全国互联网新闻信息服务的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内互联网新闻信息服务的监督管理执法工作。

第二章 许可

第五条 通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务,应当取得互联网新闻信息服务许可，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。

前款所称互联网新闻信息服务，包括互联网新闻信息采编发布服务、转载服务、传播平台服务。

第六条 申请互联网新闻信息服务许可，应当具备下列条件：

（一）在中华人民共和国境内依法设立的法人；

（二）主要负责人、总编辑是中国公民；

（三）有与服务相适应的专职新闻编辑人员、内容审核人员和技术保障人员；

（四）有健全的互联网新闻信息服务管理制度；

（五）有健全的信息安全管理制度和安全可控的技术保障措施；

（六）有与服务相适应的场所、设施和资金。

申请互联网新闻信息采编发布服务许可的，应当是新闻单位（含其控股的单位）或新闻宣传部门主管的单位。

符合条件的互联网新闻信息服务提供者实行特殊管理股制度，具体实施办法由国家互联网信息办公室另行制定。

提供互联网新闻信息服务，还应当依法向电信主管部门办理互联网信息服务许可或备案手续。

第七条 任何组织不得设立中外合资经营、中外合作经营和外资经营的互联网新闻信息服务单位。

互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报经国家互联网信息办公室进行安全评估。

第八条 互联网新闻信息服务提供者的采编业务和经营业务应当分开，非公有资本不得介入互联网新闻信息采编业务。

第九条 申请互联网新闻信息服务许可，申请主体为中央新闻单位（含其控股的单位）或中央新闻宣传部门主管的单位的，由国家互联网信息办公室受理和决定；申请主体为地方新闻单位（含其控股的单位）或地方新闻宣传部门主管的单位的，由省、自治区、直辖市互联网信息办公室受理和决定；申请主体为其他单位的，经所在地省、自治区、直辖市互联网信息办公室受理和初审后，由国家互联网信息办公室决定。

国家或省、自治区、直辖市互联网信息办公室决定批准的，核发《互联网新闻信息服务许可证》。《互联网新闻信息服务许可证》有效期为三年。有效期届满，需继续从事互联网新闻信息服务活动的，应当于有效期届满三十日前申请续办。

省、自治区、直辖市互联网信息办公室应当定期向国家互联网信息办公室报告许可受理和决定情况。

第十条 申请互联网新闻信息服务许可，应当提交下列材料：

（一）主要负责人、总编辑为中国公民的证明；

（二）专职新闻编辑人员、内容审核人员和技术保障人员的资质情况；

（三）互联网新闻信息服务管理制度；

（四）信息安全管理制度和技术保障措施；

（五）互联网新闻信息服务安全评估报告；

（六）法人资格、场所、资金和股权结构等证明；

（七）法律法规规定的其他材料。

第三章 运行

第十一条 互联网新闻信息服务提供者应当设立总编辑，总编辑对互联网新闻信息内容负总责。总编辑人选应当具有相关从业经验，符合相关条件，并报国家或省、自治区、直辖市互联网信息办公室备案。

互联网新闻信息服务相关从业人员应当依法取得相应资质，接受专业培训、考核。互联网新闻信息服务相关从业人员从事新闻采编活动，应当具备新闻采编人员职业资格，持有国家新闻出版广电总局统一颁发的新闻记者证。

第十二条 互联网新闻信息服务提供者应当健全信息发布审核、公共信息巡查、应急处置等信息安全管理制度，具有安全可控的技术保障措施。

第十三条 互联网新闻信息服务提供者为用户提供互联网新闻信息传播平台服务，应当按照《中华人民共和国网络安全法》的规定，要求用户提供真实身份信息。用户不提供真实身份信息的，互联网新闻信息服务提供者不得为其提供相关服务。

互联网新闻信息服务提供者对用户身份信息和日志信息负有保密的义务，不得泄露、篡改、毁损，不得出售或非法向他人提供。

互联网新闻信息服务提供者及其从业人员不得通过采编、发布、转载、删除新闻信息，干预新闻信息呈现或搜索结果等手段谋取不正当利益。

第十四条 互联网新闻信息服务提供者提供互联网新闻信息传播平台服务，应当与在其平台上注册的用户签订协议，明确双方权利义务。

对用户开设公众账号的，互联网新闻信息服务提供者应当审核其账号信息、服务资质、服务范围等信息，并向所在地省、自治区、直辖市互联网信息办公室分类备案。

第十五条 互联网新闻信息服务提供者转载新闻信息，应当转载中央新闻单位或省、自治区、直辖市直属新闻单位等国家规定范围内的单位发布的新闻信息，注明新闻信息来源、原作者、原标题、编辑真实姓名等，不得歪曲、篡改标题原意和新闻信息内容，并保证新闻信息来源可追溯。

互联网新闻信息服务提供者转载新闻信息，应当遵守著作权相关法律法规的规定，保护著作权人的合法权益。

第十六条 互联网新闻信息服务提供者和用户不得制作、复制、发布、传播法律、行政法规禁止的信息内容。

互联网新闻信息服务提供者提供服务过程中发现含有违反本规定第三条或前款规定内容的，应当依法立即停止传输该信息、采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第十七条 互联网新闻信息服务提供者变更主要负责人、总编辑、主管单位、股权结构等影响许可条件的重大事项，应当向原许可机关办理变更手续。

互联网新闻信息服务提供者应用新技术、调整增设具有新闻舆论属性或社会动员能力的应用功能，应当报国家或省、自治区、直辖市互联网信息办公室进行互联网新闻信息服务安全评估。

第十八条 互联网新闻信息服务提供者应当在明显位置明示互联网新闻信息服务许可证编号。

互联网新闻信息服务提供者应当自觉接受社会监督，建立社会投诉举报渠道，设置便捷的投诉举报入口，及时处理公众投诉举报。

第四章 监督检查

第十九条 国家和地方互联网信息办公室应当建立日常检查和定期检查相结合的监督管理制度，依法对互联网新闻信息服务活动实施监督检查，有关单位、个人应当予以配合。

国家和地方互联网信息办公室应当健全执法人员资格管理制度。执法人员开展执法活动，应当依法出示执法证件。

第二十条 任何组织和个人发现互联网新闻信息服务提供者有违反本规定行为的，可以向国家和地方互联网信息办公室举报。

国家和地方互联网信息办公室应当向社会公开举报受理方式，收到举报后，应当依法予以处置。互联网新闻信息服务提供者应当予以配合。

第二十一条 国家和地方互联网信息办公室应当建立互联网新闻信息服务网络信用档案，建立失信黑名单制度和约谈制度。

国家互联网信息办公室会同国务院电信、公安、新闻出版广电等部门建立信息共享机制，加强工作沟通和协作配合，依法开展联合执法等专项监督检查活动。

第五章 法律责任

第二十二条 违反本规定第五条规定，未经许可或超越许可范围开展互联网新闻信息服务活动的，由国家和省、自治区、直辖市互联网信息办公室依据职责责令停止相关服务活动，处一万元以上三万元以下罚款。

第二十三条 互联网新闻信息服务提供者运行过程中不再符合许可条件的，由原许可机关责令限期改正；逾期仍不符合许可条件的，暂停新闻信息更新；《互联网新闻信息服务许可证》有效期届满仍不符合许可条件的，不予换发许可证。

第二十四条 互联网新闻信息服务提供者违反本规定第七条第二款、第八条、第十一条、第十二条、第十三条第三款、第十四条、第十五条第一款、第十七条、第十八条规定的，由国家和地方互联网信息办公室依据职责给予警告，责令限期改正；情节严重或拒不改正的，暂停新闻信息更新，处五千元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

第二十五条 互联网新闻信息服务提供者违反本规定第三条、第十六条第一款、第十九条第一款、第二十条第二款规定的，由国家和地方互联网信息办公室依据职责给予警告，责令限期改正；情节严重或拒不改正的，暂停新闻信息更新，处二万元以上三万元以下罚款；构成犯罪的，依法追究刑事责任。

第二十六条 互联网新闻信息服务提供者违反本规定第十三条第一款、第十六条第二款规定的，由国家和地方互联网信息办公室根据《中华人民共和国网络安全法》的规定予以处理。

第六章 附则

第二十七条 本规定所称新闻单位，是指依法设立的报刊社、广播电台、电视台、通讯社和新闻电影制片厂。

第二十八条 违反本规定，同时违反互联网信息服务管理规定的，由国家和地方互联网信息办公室根据本规定处理后，转由电信主管部门依法处置。

国家对互联网视听节目服务、网络出版服务等另有规定的，应当同时符合其规定。

第二十九条 本规定自 2017 年 6 月 1 日起施行。本规定施行之前颁布的有关规定与本规定不一致的，按照本规定执行。

互联网新闻信息服务许可管理实施细则

第一条 为进一步提高互联网新闻信息服务许可管理规范化、科学化水平，促进互联网新闻信息服务健康有序发展，根据《中华人民共和国行政许可法》《互联网新闻信息服务管理规定》（以下简称《规定》），制定本细则。

第二条 国家和省、自治区、直辖市互联网信息办公室实施互联网新闻信息服务许可，适用本细则。

第三条 通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务，应当取得互联网新闻信息服务许可，禁止未经许可或超越许可范围开展互联网新闻信息服务活动。

第四条 互联网新闻信息服务，包括互联网新闻信息采编发布服务、转载服务、传播平台服务。

其中，采编发布服务，是指对新闻信息进行采集、编辑、制作并发布的服务；转载服务，是指选择、编辑并发布其他主体已发布新闻信息的服务；传播平台服务，是指为用户传播新闻信息提供平台的服务。

获准提供互联网新闻信息采编发布服务的，可以同时提供互联网新闻信息转载服务。获准提供互联网新闻信息传播平台服务，拟同时提供采编发布服务、转载服务的，应当依法取得互联网新闻信息采编发布、转载服务许可。

第五条 申请互联网新闻信息服务许可的，应当具备下列许可条件：

（一）在中华人民共和国境内依法设立的法人；

（二）主要负责人、总编辑是中国公民；

（三）有与服务相适应的专职新闻编辑人员、内容审核人员和技术保障人员；

（四）有健全的互联网新闻信息服务管理制度；

（五）有健全的信息安全管理制度和安全可控的技术保障措施；

（六）有与服务相适应的场所、设施和资金。

其中，申请互联网新闻信息采编发布服务许可的，应当是新闻单位（含新闻单位控股的单位）或新闻宣传部门主管的单位。新闻单位是指经国家有关部门依法批准设立的报刊

社、广播电台、电视台、通讯社和新闻电影制片厂。控股是指出资额、持有股份占企业资本总额或股本总额50%以上，或出资额、持有股份的比例虽然不足50%，但依其出资额或持有股份已足以对企业决议产生重大影响。新闻宣传部门包括各级宣传部门、网信部门、广电部门等。

任何组织不得设立中外合资经营、中外合作经营和外资经营的互联网新闻信息服务单位。

第六条 根据《规定》第十条，申请互联网新闻信息服务许可的，应当提交下列申请材料：

（一）主要负责人、总编辑为中国公民的证明。包括主要负责人、总编辑的身份证复印件等；

（二）专职新闻编辑人员、内容审核人员和技术保障人员的资质情况。包括相关人员基本情况，以及国家新闻出版广电总局统一颁发的新闻记者证、新闻单位从业证明、相关培训考核证明等材料，具体人员数量应当与所提供的服务相适应；

（三）互联网新闻信息服务管理制度。包括网站总编辑制度、从业人员教育培训和考核制度等；

（四）信息安全管理制度和技术保障措施。包括信息发布审核制度、公共信息巡查制度、应急处置制度、用户个人信息保护制度等，以及相关技术保障措施的情况；

（五）互联网新闻信息服务安全评估报告。由有关部门或具有相关资质的机构出具的对于申请者信息安全管理制度和技术保障措施的安全评估报告；

（六）法人资格、场所、资金的证明。包括企业营业执照、事业单位法人证书、服务场所产权证书、租赁合同等材料复印件；

（七）互联网新闻信息服务许可申请书。包括申请表，以及对拟提供具体服务形式、服务方案的说明等。

第七条 申请互联网新闻信息采编发布服务许可的,除应当提交本细则第六条规定的申请材料外，还应当提交该单位或其控股方为新闻单位的证明，或其主管单位为新闻宣传部门的证明及该主管单位的意见。其中，新闻单位证明包括《报纸出版许可证》、《广播电视播出机构许可证》、《期刊出版许可证》（持有《期刊出版许可证》的，应当以提供《规定》第二条所称“新闻信息”服务为主营业务）等；主管单位意见内容主要包括，说明申

请者与该主管单位的关系、就申请者是否符合许可条件提出评估意见并加盖单位公章等。

申请互联网新闻信息传播平台服务许可的，除应当提交本细则第六条规定的申请材料外，还应当提交平台账号用户管理规章制度、用户协议范本、投诉举报处理机制等。

申请者为企业法人的，除应当提交本细则第六条规定的申请材料外，还应当提供下列股权相关材料：

（一）股权结构图。包括股东名称、股权比例、出资方式、出资时间等信息。股东为非自然人主体的，须逐级追溯到自然人、事业单位以及国有独资公司，并就实际控制人情况作出说明。股权结构图需加盖单位公章，并由法定代表人签字；

（二）股东证明材料。股东为自然人的，须提供身份证明材料；股东为非自然人主体的，须提供该主体的名称、组织形式、法定代表人等材料；

（三）公司章程。包括公司章程及历次修改决议；

（四）无外资承诺书。申请者对股权结构图中所有股东均不含外资成分作出的书面承诺；

（五）专业机构意见书。律师事务所或会计师事务所就上述股权材料的真实性、准确性、完整性出具的书面证明，包括验资报告、法律意见书等材料。

第八条 根据《规定》第七条，互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，应当报国家互联网信息办公室进行安全评估，并提交以下材料：

（一）拟合作企业的情况。包括该企业基本情况介绍、营业执照等法人资格证明；

（二）拟合作业务的情况。包括合作意向书、合作发展规划、合作可行性分析报告等材料；

主管单位为新闻宣传部门的，还应当提交该主管单位就该项业务合作的意见。

互联网新闻信息服务单位与境内外中外合资经营、中外合作经营和外资经营的企业进行涉及互联网新闻信息服务业务的合作，可能导致互联网新闻信息服务单位不再符合许可条件的，不予通过安全评估。

第九条 国家和省、自治区、直辖市互联网信息办公室收到申请材料后，应当根据情况依法作出处理：

（一）申请材料齐全、符合要求的，予以受理；

（二）申请材料不齐全、不符合要求的，当场或五个工作日内一次性告知申请者应予更正或补充的内容；

（三）对依法不需要取得互联网新闻信息服务许可的，不予受理，并即时告知申请者，退回申请材料；

（四）对申请事项不属于职权范围的，应当即时作出不予受理的决定，并告知申请者向有关行政机关申请。

第十条 依法受理后，国家和省、自治区、直辖市互联网信息办公室按照本细则第五条、第六条、第七条的规定，对申请材料进行审核，包括申请者是否符合许可条件、材料是否真实等。

审核过程中，国家和省、自治区、直辖市互联网信息办公室可依据实际情况，约见申请者主要负责人、总编辑，到网站备案地、实际经营地、网站服务器所在地等其他相关场所进行实地检查。

第十一条 国家和省、自治区、直辖市互联网信息办公室应当依据《行政许可法》第四十二条，在规定期限内依法作出批准或不予批准的决定。批准的，核发《互联网新闻信息服务许可证》。

省、自治区、直辖市互联网信息办公室应当自作出批准决定之日起七个工作日内，向国家互联网信息办公室报告有关情况。

第十二条 根据《规定》第十七条，互联网新闻信息服务提供者变更以下事项，应当自变更之日起七个工作日内，向原许可机关申请办理变更手续：

（一）变更公司章程、服务场所、网站名称、接入服务提供者等事项；

（二）变更总编辑、主要负责人、股权结构、互联网地址等事项，或者进行上市、合并、分立；

其中，变更总编辑、主要负责人、股权结构、互联网地址等事项，或者进行上市、合并、分立，导致互联网新闻信息服务提供者不再符合许可条件的，根据《规定》第二十三条予以处罚。

互联网新闻信息服务提供者新增服务类别，应当根据《规定》第六条，依法取得相应的许可。

第十三条 互联网新闻信息服务提供者申请办理本细则第十二条相关变更手续，应当向

原许可机关提交以下材料：

（一）变更申请书。包括申请变更事项、变更原因以及其他需要说明的问题，并加盖单位公章；

（二）变更事项材料。提交具体变更事项的说明、证明材料，包括变更人员基本情况、资格证书、任免证明，或者变更后的营业执照、公司章程、租赁合同等，并加盖单位公章。

变更股权结构的，应当按照本细则第七条规定，提供相关股权材料。涉及上市的，还应当提供有关上市活动具体实施方案、新三板挂牌方案以及战略投资机构有关情况等材料。

涉及许可证所列事项变更的，应当提交许可证原件。

第十四条 《互联网新闻信息服务许可证》有效期为三年。有效期届满，需继续从事互联网新闻信息服务活动的，应当于有效期届满三十日前，按照许可程序，向原许可机关申请续办，并提交以下材料：

（一）许可续办申请书。包括前期从业情况说明、涉及本细则第五条许可条件相关情况的说明，以及其他需要说明的问题，并加盖单位公章；

（二）许可证原件。

主管单位为新闻宣传部门的，还应当提交该主管单位的意见。

《互联网新闻信息服务许可证》有效期届满，未依法申请续办的，不得继续提供互联网新闻信息服务，原许可证作废。

第十五条 根据《行政许可法》第九条，互联网新闻信息服务许可不得转让。互联网新闻信息服务提供者不得因业务调整、合并、分立等原因擅自转让许可。

第十六条 互联网新闻信息服务提供者终止服务的，应当自终止服务之日起三十日内向原许可机关办理注销手续，并提交以下材料：

（一）注销申请书。包括注销原因以及其他需要说明的问题，并加盖单位公章；

（二）许可证原件。

第十七条 根据《规定》第十九条，国家和地方互联网信息办公室建立抽查、考核等日常检查和定期检查相结合的监督管理制度，加强对互联网新闻信息服务活动的监督检查，有关单位、个人应当予以配合。

监督检查结果，依法向社会公开，接受社会监督。

第十八条 本细则与《规定》同步施行。

国家网络安全检查操作指南

中央网络安全和信息化领导小组办公室

网络安全协调局

2016 年 6 月

目　录

国家网络安全检查操作指南

为指导关键信息基础设施网络安全检查工作，依据《关于开展关键信息基础设施网络安全检查的通知》（中网办发〔2016〕3号，以下简称《检查通知》），参照《信息安全技术 政府部门信息安全管理基本要求》（GB/T 29245-2012）等国家网络安全技术标准规范，制定本指南。

本指南主要用于各地区、各部门、各单位在开展关键信息基础设施网络安全检查工作（以下简称“检查工作”）时参考。

1 概述

1.1 检查目的

为贯彻落实习近平总书记关于“加快构建关键信息基础设施安全保障体系”，“全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”的重要指示精神，摸清关键信息基础设施底数，掌握关键信息基础设施风险和防护状况，以查“促建、促管、促改、促防”，推动建立关键信息基础设施网络安全责任制和防范体系，保障关键信息基础设施的安全稳定运行。

1.2 检查工作流程

检查工作流程通常包括检查工作部署、关键信息基础设施摸底、网络安全检查、检查总结整改四个步骤。

其中，网络安全检查包括信息系统基本情况检查、网络安全责任制落实情况检查、网络安全日常管理情况检查、网络安全防护情况检查、网络安全应急工作情况检查、网络安全教育培训情况检查、技术检测及网络安全事件情况检查、信息技术外包服务机构情况检查等八个环节，如下图所示。

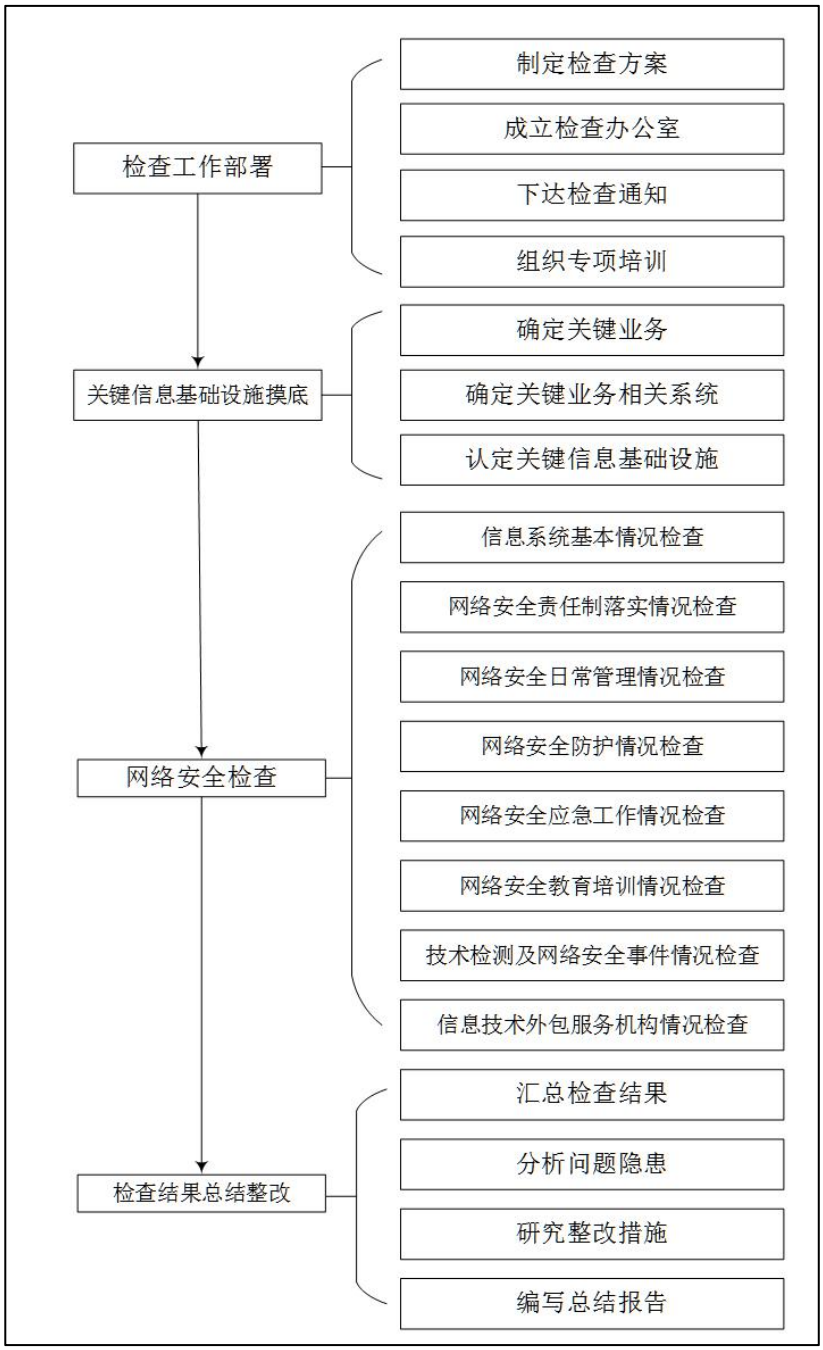


图1 网络安全检查工作流程图

2 检查工作部署

检查工作部署通常包括研究制定检查方案、成立检查办公室、下达检查通知等具体工作。

2.1 研究制定检查方案

本单位网络安全管理部门根据《检查通知》统一安排，结合工作实际，制定检查方案，并报本单位网络安全主管领导批准。

检查方案应当明确以下内容：（1）检查工作负责人、组织机构和具体实施机构；（2）检查范围和检查重点；（3）检查内容；（4）检查工作组织开展方式；（5）检查工作时间进度安排；（6）有关工作要求。

1. 关于检查范围。检查的范围通常包括本单位各内设机构，以及为本单位信息系统（包括网站系统、平台系统、生产业务系统等）提供运行维护支撑服务的下属单位。可根据本单位网络安全保障工作需要，将其他为本单位信息系统提供运维服务、对本单位信息系统安全可能产生重大影响的相关单位纳入检查范围。

2. 关于检查重点。在对各类信息系统进行全面检查的基础上，应突出重点，对事关国家安全和社会稳定，对地区、部门或行业正常生产生活具有较大影响的关键信息基础设施进行重点检查。

3. 关于关键信息基础设施确定，应结合本单位实际，参考《关于开展关键信息基础设施网络安全检查的通知》中的《关键信息基础设施确定指南》进行确定。

2.2 成立检查办公室

本单位网络安全管理部门制定完成检查方案后，应及时成立检查办公室，明确人员、经费和技术保障；组织开展培训，保证办公室成员熟悉检查方案，掌握检查内容、填报工具使用方法等。

办公室成员通常由网络安全管理及运维部门、信息化部门有关人员，相关业务部门中熟悉业务、具备网络安全知识的人员，以及本单位相关技术支撑机构的业务骨干等组成。

对于网络与信息系统复杂、检查工作涉及部门多的单位，可根据需要成立检查工作领导小组，负责检查工作的组织协调与资源配置。领导小组组长可由本单位主要负责同志担任，领导小组成员可包括网络安全管理机构负责人（如办公厅主任）、信息化部门负责人（如信息中心主任），以及其他相关部门负责人（如人事部门、财务部门、业务部门领导）等。

2.3 下达检查通知

本单位网络安全管理部门应以书面形式部署关键信息基础设施网络安全检查工作，明确检查时间、检查范围、检查内容、工作要求等具体事项。

2.4 组织专项培训

本单位要组织专项培训，对本单位负责检查工作的干部、专家、技术人员、有关关键信息基础设施运维人员等进行广泛培训，确保检查工作质量，培训内容应包括检查目的意义、流程方法、关键信息基础设施确定方法及登记表填报说明、网络安全检查方法等。

3 关键信息基础设施摸底

3.1 关键信息基础设施定义及范围

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括网站类，如党政机关网站、企事业单位网站、新闻网站等；平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

3.2 确定关键信息基础设施步骤

关键信息基础设施的确定，通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

（一）确定本地区、本部门、本行业的关键业务。

可参考表1，结合本地区、本部门、本行业实际梳理关键业务。

表1 关键信息基础设施业务判定表

行业		关键业务
能源	电力	● 电力生产（含火电、水电、核电等） ● 电力传输 ● 电力配送
	石油石化	● 油气开采 ● 炼化加工 ● 油气输送 ● 油气储存
	煤炭	● 煤炭开采 ● 煤化工
金融		● 银行运营 ● 证券期货交易 ● 清算支付 ● 保险运营
交通	铁路	● 客运服务 ● 货运服务 ● 运输生产 ● 车站运行
	民航	● 空运交通管控 ● 机场运行 ● 订票、离港及飞行调度检查安排 ● 航空公司运营
	公路	● 公路交通管控 ● 智能交通系统（一卡通、ETC 收费等）
	水运	● 水运公司运营（含客运、货运）

		● 港口管理运营 ● 航运交通管控
水利		● 水利枢纽运行及管控 ● 长距离输水管控 ● 城市水源地管控
医疗卫生		● 医院等卫生机构运行 ● 疾病控制 ● 急救中心运行
环境保护		● 环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）		● 企业运营管理 ● 智能制造系统（工业互联网、物联网、智能装备等） ● 危化品生产加工和存储管控（化学、核等） ● 高风险工业设施运行管控
市政		● 水、暖、气供应管理 ● 城市轨道交通 ● 污水处理 ● 智慧城市运行及管控
电信与互联网		● 语音、数据、互联网基础网络及枢纽 ● 域名解析服务和国家顶级域注册管理 ● 数据中心/云服务
广播电视		● 电视播出管控 ● 广播播出管控
政府部门		● 信息公开 ● 面向公众服务 ● 办公业务系统
行业		关键业务
能源	电力	● 电力生产（含火电、水电、核电等） ● 电力传输 ● 电力配送
	石油石化	● 油气开采 ● 炼化加工 ● 油气输送 ● 油气储存
	煤炭	● 煤炭开采 ● 煤化工
金融		● 银行运营 ● 证券期货交易 ● 清算支付 ● 保险运营
交通	铁路	● 客运服务 ● 货运服务 ● 运输生产 ● 车站运行
	民航	● 空运交通管控 ● 机场运行 ● 订票、离港及飞行调度检查安排 ● 航空公司运营
	公路	● 公路交通管控 ● 智能交通系统（一卡通、ETC 收费等）
	水运	● 水运公司运营（含客运、货运） ● 港口管理运营

	● 航运交通管控
水利	● 水利枢纽运行及管控 ● 长距离输水管控 ● 城市水源地管控
医疗卫生	● 医院等卫生机构运行 ● 疾病控制 ● 急救中心运行
环境保护	● 环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）	● 企业运营管理 ● 智能制造系统（工业互联网、物联网、智能装备等） ● 危化品生产加工和存储管控（化学、核等） ● 高风险工业设施运行管控
市政	● 水、暖、气供应管理 ● 城市轨道交通 ● 污水处理 ● 智慧城市运行及管控
电信与互联网	● 语音、数据、互联网基础网络及枢纽 ● 域名解析服务和国家顶级域注册管理 ● 数据中心/云服务
广播电视	● 电视播出管控 ● 广播播出管控
政府部门	● 信息公开 ● 面向公众服务 ● 办公业务系统

（二）确定关键业务相关的信息系统或工业控制系统。

根据关键业务，逐一梳理出支撑关键业务运行或与关键业务相关的信息系统或工业控制系统，形成候选关键信息基础设施清单。如电力行业火电企业的发电机组控制系统、管理信息系统等；市政供水相关的水厂生产控制系统、供水管网监控系统等。

（三）认定关键信息基础设施。

对候选关键信息基础设施清单中的信息系统或工业控制系统，根据本地区、本部门、本行业实际，参照以下标准认定关键信息基础设施。

A.网站类

符合以下条件之一的，可认定为关键信息基础设施：

1. 县级（含）以上党政机关网站。（2016年检查中，所有党政机关网站均应填写上报登记表）

2. 重点新闻网站。（2016年检查中，所有新闻网站均应填写上报登记表）

3. 日均访问量超过100万人次的网站。

4. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）影响超过100万人工作、生活；

（2）影响单个地市级行政区30%以上人口的工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害政府形象、社会秩序，或危害国家安全。

5. 其他应该认定为关键信息基础设施。

B.平台类

符合以下条件之一的，可认定为关键信息基础设施：

1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。

2. 日均成交订单额或交易额超过1000万元。

3. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）造成1000万元以上的直接经济损失；

（2）直接影响超过1000万人工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害社会和经济秩序，或危害国家安全。

4.其他应该认定为关键信息基础设施。

C.生产业务类

符合以下条件之一的，可认定为关键信息基础设施：

1. 地市级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。

2. 规模超过1500个标准机架的数据中心。

3. 一旦发生安全事故，可能造成以下影响之一的：

（1）影响单个地市级行政区30%以上人口的工作、生活；

（2）影响10万人用水、用电、用气、用油、取暖或交通出行等；

（3）导致5人以上死亡或50人以上重伤；

（4）直接造成5000万元以上经济损失；

（5）造成超过100万人个人信息泄露；

（6）造成大量机构、企业敏感信息泄露；

（7）造成大量地理、人口、资源等国家基础数据泄露；

（8）严重损害社会和经济秩序，或危害国家安全。

4.其他应该认定为关键信息基础设施。

3.3 关键信息基础设施信息登记

各单位梳理确定本单位所主管的关键信息基础设施，并通过填报工具填写登记表。主要包括：

a）设施主管单位信息；

b）设施主要负责人、网络安全管理部门负责人、运维单位负责人联系方式；

c）设施提供服务的基本类型、功能描述、网页入口信息、发生网络安全事故后影响分析、投入情况、信息技术产品国产化率；

e）数据存储情况；

f）运行环境情况；

g）运行维护情况；

h）网络安全状况；

i）商用密码使用情况。

填报工具的使用，详见《国家网络安全检查信息共享平台及关键信息基础设施填报工具使用手册》

4 网络安全检查

4.1 网络安全责任制落实情况检查

网络安全责任制落实情况检查通常包括网络安全管理工作单位领导、网络安全管理工作内设机构、网络安全责任制度建设和落实情况的检查。

4.2.1 要求

a）应明确一名主管领导，负责本单位网络安全管理工作，根据国家法律法规有关要求，结合实际组织制定网络安全管理制度，完善技术防护措施，协调处理重大网络安全事件；

b）应指定一个机构，具体承担网络安全管理工作，负责组织落实网络安全管理制度和网络安全技术防护措施，开展网络安全教育培训和监督检查等；

c）应建立健全岗位网络安全责任制度，明确岗位及人员的网络安全责任。

4.2.2 检查方式

文档查验、人员访谈。

4.2.3 检查方法

a）查验领导分工等文件，检查是否明确了网络安全主管领导；查验网络安全相关工作批示、会议记录等，了解主管领导履职情况；

b）查验本单位各内设机构职责分工等文件，检查是否指定了网络安全管理机构（如工业和信息化部指定办公厅为网络安全管理机构）；

c）查验工作计划、工作方案、规章制度、监督检查记录、教育培训记录等文档，了解管理机构履职情况；

d）查验岗位网络安全责任制度文件，检查系统管理员、网络管理员、网络安全员、一般工作人员等不同岗位的网络安全责任是否明确；

e）访谈关键岗位网络安全员，检查其网络安全意识和网络安全知识、技能掌握情况；

f）查验工作计划、工作报告等相关文档，检查网络安全员日常工作开展情况。

表2 网络安全责任制落实情况检查表

负责网络安全管理工作的单位领导	①负责网络安全管理工作的领导：□已明确 □未明确 ②姓名：_____ ③职务：_____ ④是否本单位主要负责同志：□是 □否
负责网络安全管理的内设机构	①负责网络安全管理的内设机构：□已明确 □未明确 ②机构名称：_____ ③负责人：_____职 务：_____

	④联系人：_____办公电话：_____ 移动电话：_____
网络安全责任制度建设和落实情况	①网络安全责任制度：□已建立 □未建立 ②网络安全检查责任：□已明确 □未明确 ③本年度网络安全检查专项经费：□已落实，_____万 □无专项经费

4.2 网络安全日常管理情况检查

4.3.1 人员管理检查

4.3.1.1 要求

a）应与重点岗位的计算机使用和管理人员签订网络安全与保密协议，明确网络安全与保密要求和责任；

b）应制定并严格执行人员离岗离职网络安全管理规定，人员离岗离职时应终止信息系统访问权限，收回各种软硬件设备及身份证件、门禁卡等，并签署安全保密承诺书；

c）应建立外部人员访问机房等重要区域审批制度，外部人员须经审批后方可进入，并安排本单位工作人员现场陪同，对访问活动进行记录并留存；

d）应对网络安全责任事故进行查处，对违反网络安全管理规定的人员给予严肃处理，对造成网络安全事故的依法追究当事人和有关负责人的责任，并以适当方式通报。

4.3.1.2 检查方式

文档查验、人员访谈。

4.3.1.3 检查方法

a）查验岗位网络安全责任制度文件，检查系统管理员、网络管理员、网络安全员、一般工作人员等不同岗位的网络安全责任是否明确；检查重点岗位人员网络安全与保密协议签订情况；访谈部分重点岗位人员，抽查对网络安全责任的了解程度；

b）查验人员离岗离职管理制度文件，检查是否有终止系统访问权限、收回软硬件设备、收回身份证件和门禁卡等要求；检查离岗离职人员安全保密承诺书签署情况；查验信息系统账户，检查离岗离职人员账户访问权限是否已被终止；

c）查验外部人员访问机房等重要区域的审批制度文件，检查是否有访问审批、人员陪同等要求；查验访问审批记录、访问活动记录，检查记录是否清晰、完整；

d）查验安全事件记录及安全事件责任查处等文档，检查是否发生过因违反制度规定造成的网络安全事件、是否对网络安全事件责任人进行了处置。

表3 人员管理检查结果记录表

人员管理	①重点岗位人员安全保密协议：□全部签订 □部分签订 □均未签订 ②人员离岗离职安全管理规定：□已制定 □未制定

	③外部人员访问机房等重要区域审批制度：□已建立 □未建立

4.3.2 信息资产管理情况检查

4.3.2.1 要求

a）应建立并严格执行信息资产管理制度；

b）应指定专人负责信息资产管理；

c）应建立信息资产台账（清单），统一编号、统一标识、统一发放；

d）应及时记录信息资产状态和使用情况，保证账物相符；

e）应建立并严格执行设备维修维护和报废管理制度。

4.3.2.2 检查方式

文档查验、人员访谈。

4.3.2.3 检查方法

a）查验信息资产管理制度文档，检查信息资产管理制度是否建立；

b）查验设备管理员任命及岗位分工等文件，检查是否明确专人负责信息资产管理；访谈设备管理员，检查其对信息资产管理制度和日常工作任务的了解程度；

c）查验信息资产台账，检查台账是否完整（包括设备编号、设备状态、责任人等信息）；查验领用记录，检查是否做到统一编号、统一标识、统一发放；

d）随机抽取台账中的部分设备登记信息，查验是否有对应的实物；随机抽取一定数量的实物，查验其是否纳入信息资产台账，同台账是否相符；

e）查验相关制度文档和记录，检查设备维修维护和报废管理制度建立及落实情况。

表4 信息资产管理检查记录表

信息资产管理	①信息资产管理制度：□已建立 □未建立 ②设备维修维护和报废管理： □已建立管理制度，且记录完整 □已建立管理制度，但记录不完整 □未建立管理制度

4.3.3 经费保障情况检查

4.3.3.1 要求

a）应将网络安全设施运行维护、网络安全服务采购、日常网络安全管理、网络安全教育培训、网络安全检查、网络安全风险评估、网络安全应急处置等费用纳入部门年度预算；

b）应严格落实网络安全经费预算，保证网络安全经费投入。

4.3.3.2 检查方式

文档查验。

4.3.3.3 检查方法

a）会同本单位财物部门人员，查验上一年度和本年度预算文件，检查年度预算中是否有网络安全相关费用；

b）查验相关财务文档和经费使用账目，检查上一年度网络安全经费实际投入情况、网络安全经费是否专款专用。

表5 经费保障检查结果记录表

经费保障	①上一年度信息化总投入：_____万元，网络安全实际投入：_____万元，其中采购网络安全服务比例：_____ ②本年度信息化总预算（含网络安全预算）：_____万元，网络安全预算：_____万元，其中采购网络安全服务比例：_____

4.3 信息系统基本情况检查

对本单位主管信息系统进行全面检查，及时掌握本单位信息系统基本情况，特别是变更情况，以便针对性地开展网络安全管理和防护工作。

4.1.1 基本信息梳理

查验信息系统规划设计方案、安全防护规划设计方案、网络拓扑图等相关文档，访谈信息系统管理人员与工作人员，了解掌握系统基本信息并记录结果（表6），包括：

a）主要功能、部署位置、网络拓扑结构、服务对象、用户规模、业务周期、运行高峰期等；

b）业务主管部门、运维机构、系统开发商和集成商、上线运行及系统升级日期等；

c）定级情况、数据集中情况、灾备情况等。

表6 系统基本信息梳理记录表（每个系统一张表）

编号	
系统名称	
主要功能	
部署位置	
网络拓扑结构	

服务对象	
用户规模	
业务周期	
业务主管部门	
运维机构	
系统开发商	
系统集成商	
上线运行及最近一次系统升级时间	
定级情况	
数据集中情况	
灾备情况	

4.1.2 系统构成情况梳理

4.1.2.1 主要硬件构成

重点梳理主要硬件设备类型、数量、生产商（品牌）情况，记录结果（表7）。

硬件设备类型主要有：服务器、终端计算机、路由器、交换机、存储设备、防火墙、终端计算机、磁盘阵列、磁带库及其他主要安全设备。

表7 信息系统主要硬件构成梳理记录表

<table>
<tr><td>检查项</td><td colspan="9">检查结果</td></tr>
<tr><td rowspan="3">服务器</td><td>品牌</td><td>联想</td><td>曙光</td><td>浪潮</td><td>华为</td><td>IBM</td><td>HP</td><td>ELL</td><td>racle</td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="9">其他：
1. 品牌 ，数量
2. 品牌 ，数量
①使用国产 CPU 的台数：
②使用国产操作系统的台数：</td></tr>
<tr><td rowspan="3">终端计算机
（含笔记本）</td><td>品牌</td><td>联想</td><td>长城</td><td>方正</td><td>清华同方</td><td>华硕</td><td>宏基</td><td></td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">其他：
1. 品牌 ，数量
2. 品牌 ，数量
①使用国产 CPU 的台数
②使用国产操作系统的台数：
使用 Windows xp/7/8 的台数：</td></tr>
</table>

<table>
<tr><td></td><td colspan="7">③安装国产字处理软件的台数：
④安装国产防病毒软件的台数：</td></tr>
<tr><td rowspan="3">路由器</td><td>品牌</td><td>华为</td><td>中兴</td><td>锐捷网络</td><td>H3C</td><td>Cisco</td><td>Juniper</td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="7">其他：
1. 品牌 ，数量
2. 品牌 ，数量</td></tr>
<tr><td rowspan="3">交换机</td><td>品牌</td><td>华为</td><td>中兴</td><td>锐捷网络</td><td>H3C</td><td>Cisco</td><td>Juniper</td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="7">其他：
1. 品牌 ，数量
2. 品牌 ，数量</td></tr>
<tr><td>存储设备</td><td colspan="7">总台数：
1. 品牌 ，数量
2. 品牌 ，数量</td></tr>
<tr><td>防火墙</td><td colspan="7">1. 品牌 ，数量
2. 品牌 ，数量
（如有更多，可另列表）</td></tr>
<tr><td>负载均衡设备</td><td colspan="7">1. 品牌 ，数量
2. 品牌 ，数量
（如有更多，可另列表）</td></tr>
<tr><td>入侵检测设备（入侵防御）</td><td colspan="7">1. 品牌 ，数量
2. 品牌 ，数量
（如有更多，可另列表）</td></tr>
<tr><td>安全审计设备</td><td colspan="7">1. 品牌 ，数量
2. 品牌 ，数量
（如有更多，可另列表）</td></tr>
<tr><td>其 他</td><td colspan="7">1. 设备类型： ，品牌 ，数量
2. 设备类型： ，品牌 ，数量
（如有更多，可另列表）</td></tr>
</table>

4.1.2.2 主要软件构成

重点梳理主要软件类型、套数、生产商（品牌）情况，记录结果（表8）。

软件类型主要有：操作系统、数据库管理系统、公文处理软件、邮件系统及主要业务应用系统。

表8 信息系统主要软件构成梳理记录表

<table>
<tr><td>检查项</td><td colspan="8">检查结果</td></tr>
<tr><td rowspan="3">操作系统</td><td>品牌</td><td>红旗</td><td>麒麟</td><td>Windows</td><td>RedHat</td><td>HP-Unix</td><td>AIX</td><td>Solaris</td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">其他：
1. 品牌 ，数量
2. 品牌 ，数量
（如有更多，可另列表）</td></tr>
<tr><td rowspan="3">数据库管理系统</td><td>品牌</td><td>金仓</td><td>达梦</td><td>Oracle</td><td>DB2</td><td>SQLServer</td><td>Access</td><td>Mysql</td></tr>
<tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">其他：
1. 品牌 ，数量
2. 品牌 ，数量</td></tr>
<tr><td rowspan="2">公文处理软件</td><td>品牌</td><td colspan="2"></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>数量</td><td colspan="2"></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>邮件系统</td><td colspan="8">总数：
1. 品牌 ，数量
2. 品牌 ，数量</td></tr>
<tr><td>其 他</td><td colspan="8">1. 设备类型： ，品牌 ，数量
2. 设备类型： ，品牌 ，数量
（如有更多，可另列表）</td></tr>
</table>

4.4 网络安全技术防护情况检查

4.4.1 网络边界安全防护情况检查

4.4.1.1 要求

a）非涉密信息系统与互联网及其他公共信息网络应实行逻辑隔离，涉密信息系统与互联网及其他公共信息网络应实行物理隔离；

b）建立互联网接入审批和登记制度，严格控制互联网接入口数量，加强互联网接入口安全管理和安全防护；

c）应采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等措施，进行网络边界防护；

d）应根据承载业务的重要性对网络进行分区分域管理，采取必要的技术措施对不同网络分区进行防护、对不同安全域之间实施访问控制；

e）应对网络日志进行管理，定期分析，及时发现安全风险。

4.4.1.2 检查方式

文档查验、现场核查。

4.4.1.3 检查方法

a）查验网络拓扑图，检查重要设备连接情况，现场核查内部办公系统等非涉密系统的交换机、路由器等网络设备，确认以上设备的光纤、网线等物理线路没有与互联网及其他公共信息网络直接连接，有相应的安全隔离措施；

b）查验网络拓扑图，检查接入互联网情况，统计网络外联的出口个数，检查每个出口是否均有相应的安全防护措施（互联网接入口指内部网络与公共互联网边界处的接口，如联通、电信等提供的互联网接口，不包括内部网络与其他非公共网络连接的接口）；

c）查验网络拓扑图，检查是否在网络边界部署了访问控制（如防火墙）、入侵检测、安全审计以及非法外联检测、病毒防护等必要的安全设备；

d）分析网络拓扑图，检查网络隔离设备部署、交换机 VLAN 划分情况，检查网络是否按重要程度划分了安全区域，并确认不同区域间采用了正确的隔离措施；

e）查验网络日志（重点是互联网访问日志）及其分析报告，检查日志分析周期、日志保存方式和保存时限等。

表9 网络边界安全防护检查结果记录表

网络边界安全防护	①网络安全防护设备部署（可多选）： □防火墙　□入侵检测设备　□安全审计设备 □防病毒网关　□抗拒绝服务攻击设备 □Web 应用防火墙 □其它

	②设备安全策略配置：□使用默认配置　　□根据需要配置 ③网络访问日志：□留存日志　□未留存日志

4.4.2 无线网络安全防护情况检查

4.4.2.1 要求

a）采取身份鉴别、地址过滤等措施对无线网络的接入进行管理，采用白名单管理机制，防止非授权接入造成的内网渗透事件发生；

b）修改无线路由设备的默认管理地址；

c）修改无线路由管理账户默认口令，设置复杂口令，防止暴力破解后台；

d）用户接入认证加密采用 WPA2 及更高级别算法，防止破解接入口令。

4.4.2.2 检查方式

现场核查。

4.4.2.3 检查方法

a）登录无线设备管理页面，查看加密方认证方式是否采用 WPA2 以上；

b）检查用户接入认证及管理端口登录口令，包括口令强度和更新频率，查看是否登录页面采用默认地址及默认口令；

c）登录无线网络设备管理端，检查安全防护策略配置情况，包括是否设置对接入设备采取身份鉴别认证措施和地址过滤措施；

表10 无线网络安全防护情况检查结果记录表

无线网络 安全防护	①本单位使用无线路由器数量： ②无线路由器用途： □访问互联网：　　个 □访问业务/办公网络：　　个 ③安全防护策略（可多选）： □采取身份鉴别措施　□采取地址过滤措施 □未设置安全防护策略 ④无线路由器使用默认管理地址情况：□存在　□不存在 ⑤无线路由器使用默认管理口令情况：□存在　□不存在

4.4.3 电子邮件系统安全防护情况检查

4.4.3.1 要求

a）应加强电子邮件系统安全防护，采取反垃圾邮件等技术措施；

b）应规范电子邮箱的注册管理，原则上只限于本部门工作人员注册使用；

c）应严格管理邮箱账户及口令，采取技术和管理措施确保口令具有一定强度并定期更换。

4.4.3.2 检查方式

文档查验、现场核查。

4.4.3.3 检查方法

a）查验电子邮件系统采购合同或部署文档，检查电子邮件系统建设方式；

b）查验电子邮件系统管理相关规定文档，检查是否有注册审批流程要求；查验服务器上邮箱账户列表，同本单位人员名单进行核对，检查是否有非本单位人员使用；

c）查看邮箱口令策略配置界面，检查电子邮件系统是否设置了口令策略，是否对口令强度和更改周期等进行要求。

d）查验设备部署或配置情况，检查电子邮件系统是否采取了反垃圾邮件、病毒木马防护等技术安全防护措施；

表11 电子邮件系统安全防护检查结果记录表

电子邮件安全防护	①建设方式：□自行建设 □由上级单位统一管理 □使用第三方服务　邮件服务提供商 ②帐户数量：　　个 ③注册管理：□须经审批登记　□任意注册 ④注销管理：□人员离职后，及时注销　　□无管理措施 ⑤口令管理：□使用技术措施控制口令强度 位数要求：□4 位　□6 位　□8 位　其他： 复杂度要求：□数字　□字母　□特殊字符 更换频次要求：□强制定期更换，更换频次： □无强制更换要求 □没有采取技术措施控制口令强度 ⑥安全防护：（可多选） □采取数字证书 □采取反垃圾邮件措施 □其他：

4.4.4 终端计算机安全防护情况检查

4.4.4.1 要求

a）应采用集中统一管理方式对终端计算机进行管理，统一软件下发，统一安装系统补丁，统一实施病毒库升级和病毒查杀，统一进行漏洞扫描；

b）应规范软硬件使用，不得擅自更改软硬件配置，不得擅自安装软件；

c）应加强账户及口令管理，使用具有一定强度的口令并定期更换；

d）应对接入互联网的终端计算机采取控制措施，包括实名接入认证、IP 地址与 MAC 地址绑定等；

e）应定期对终端计算机进行安全审计；

f）非涉密计算机不得存储和处理国家秘密信息。

4.4.4.2 检查方式

现场核查、工具检测。

4.4.4.3 检查方法

a）查看集中管理服务器，抽查终端计算机，检查是否部署了终端管理系统或采用了其他集中统一管理方式对终端计算机进行管理，包括统一软硬件安装、统一补丁升级、统一病毒防护、统一安全审计等；

b）查看终端计算机，检查是否安装有与工作无关的软件；

c）使用终端检查工具或采用人工方式，检查终端计算机是否配置了口令策略；

d）访谈网络管理员和工作人员，检查是否采取了实名接入认证、IP 地址与 MAC 地址绑定等措施对接入本单位网络的终端计算机进行控制;将未经授权的终端计算机接入网络,测试是否能够访问互联网，验证控制措施的有效性；

e）查验审计记录，检查是否对终端计算机进行了安全审计。

表12终端计算机安全防护检查结果记录表

终端计算机安全防护	①管理方式： □集中统一管理（可多选） □规范软硬件安装　□统一补丁升级　□统一病毒防护 □统一安全审计　□对移动存储介质接入实施控制 □统一身份管理 □分散管理 ②接入互联网安全控制措施： □有控制措施（如实名接入、绑定计算机 IP 和 MAC 地址等） □无控制措施 ③接入办公系统安全控制措施： □有控制措施（如实名接入、绑定计算机 IP 和 MAC 地址等） □无控制措施

4.4.5 移动存储介质检查

4.4.5.1 要求

a）应严格存储阵列、磁带库等大容量存储介质的管理，采取技术措施防范外联风险，确保存储数据安全；

b）应对移动存储介质进行集中统一管理，记录介质领用、交回、维修、报废、销毁等情况；

c）非涉密移动存储介质不得存储涉及国家秘密的信息，不得在涉密计算机上使用；

d）移动存储介质在接入本部门计算机和信息系统前，应当查杀病毒、木马等恶意代码；

e）应配备必要的电子信息消除和销毁设备，对变更用途的存储介质要消除信息，对废弃的存储介质要进行销毁。

4.4.5.2 检查方式

文档查验、人员访谈、现场核查。

4.4.5.3 检查方法

a）访谈网络管理员，检查大容量存储介质是否存在远程维护，对于有远程维护的，进一步检查是否有相应的安全风险控制措施；查看光纤、网线等物理线路连接情况，检查大容量存储介质是否在无防护措施情况下与互联网及其他公共信息网络直接连接；

b）查验相关记录，检查是否对移动存储介质进行统一管理，包括统一领用、交回、维修、报废、销毁等；

c）查看服务器和办公终端计算机上的杀毒软件，检查是否开启了移动存储介质接入自动查杀功能；

d）查看设备台账或实物，检查是否配备了电子信息消除和销毁设备。

表13 存储介质安全防护检查结果记录表

移动存储介质安全防护	①管理方式： □集中管理，统一登记、配发、收回、维修、报废、销毁 □未采取集中管理方式 ②信息销毁： □已配备信息消除和销毁设备　□未配备信息消除和销毁设备

4.4.6 漏洞修复情况检查

4.4.6.1 要求

a）应定期对本单位主机、网络安全防护设备、信息系统进行漏洞检测，对于发现的安全漏洞及时进行修复处置；

b）重视自行监测发现与第三方漏洞通报机构告知的漏洞风险，及时处置。

4.4.6.2 检查方法

人员访谈、现场核查

4.4.6.3 检查要求

a）查看相关漏洞扫描记录，确定扫描时间和周期；

b）查验收到的漏洞风险通报，访谈网站安全管理人员是否对漏洞风险进行及时处置；

c）查验事件处置记录，检查网络安全事件报告和通报机制建立情况，是否对所有网络安全事件都进行了处置。

表14 漏洞修复情况检查结果记录表

漏洞修复情况	①漏洞检测周期：□每月 □每季度 □每年 □不进行漏洞检测 ②2015 年自行发现漏洞数量： 个 收到漏洞风险通报数量： 个 其中已得到处置的漏洞风险数量： 个

4.5 网络安全应急工作情况检查

4.5.1 要求

a）应制定网络安全事件应急预案，原则上每年评估一次，并根据实际情况适时修订；

b）应组织开展应急预案的宣贯培训，确保相关人员熟悉应急预案；

c）每年应开展网络安全应急演练，检验应急预案的可操作性，并将演练情况报网络安全主管部门；

d）应建立网络安全事件报告和通报机制，提高预防预警能力；

e）应明确应急技术支援队伍，做好应急技术支援准备；

f）应做好网络安全应急物资保障，确保必要的备机、备件等资源到位；

g）应根据业务实际需要对重要数据和业务系统进行备份。

4.5.2 检查方式

文档查验、人员访谈。

4.5.3 检查方法

a）查验应急预案文本等，检查应急预案制定和年度评估修订情况；

b）查验宣贯材料和培训记录，检查是否开展过预案宣贯培训；访谈系统管理员、网络管理员和工作人员，检查其对应急预案的熟悉程度；

c）查验演练计划、方案、记录、总结等文档，检查本年度是否开展了应急演练；

d）查验事件处置记录，检查网络安全事件报告和通报机制建立情况，是否对所有网络安全事件都进行了处置；

e）查验应急技术支援队伍合同及安全协议、参与应急技术演练及应急响应等工作的记录文件，确认应急技术支援队伍能够发挥有效的应急技术支撑作用；

f）查验设备或采购协议，检查是否有网络安全应急保障物资或有供应渠道；

g）查验备份数据和备份系统，检查是否对重要数据和业务系统进行了备份。

表15 网络安全应急工作检查结果记录表

应急预案	□已制定　　2015 年修订情况：□修订　　□未修订 □未制定
	2015 年应急预案启动次数：
应急演练	□2015 年已开展，演练次数：　　，其中实战演练数： □2015 年未开展
应急技术队伍	□本部门所属　　□外部服务机构　　□无

4.6 网络安全教育培训情况检查

4.6.1 要求

a）应加强网络安全宣传和教育培训工作，提高网络安全意识，增强网络安全基本防护技能；

b）应定期开展网络安全管理人员和技术人员专业技能培训，提高网络安全工作能力和水平；

c）应记录并保存网络安全教育培训、考核情况和结果。

4.6.2 检查方式

文档查验、人员访谈。

4.6.3 检查方法

a）查验教育宣传计划、会议通知、宣传资料等文档，检查网络安全形势和警示教育、基本防护技能培训开展情况；

b）访谈机关工作人员，检查网络安全基本防护技能掌握情况；

c）查验培训通知、培训教材、结业证书等，检查网络安全管理和技术人员专业技能培训情况。

表16 网络安全教育培训检查结果记录表

培训次数	2015 年开展网络安全教育培训（非保密培训）的次数：_____
培训人数	2015 年参加网络安全教育培训的人数：_____ 占本单位总人数的比例：_____%

4.7 技术检测及网络安全事件情况

4.7.1 技术检测情况

4.7.1.1 渗透测试

a）应重点对认定为关键信息基础设施的信息系统进行安全检测；

b）使用漏洞扫描等工具测试关键信息基础设施，检测是否存在安全漏洞；

c）开展人工渗透测试，检查是否可以获取应用系统权限，验证网站是否可以被挂马、篡改页面、获取敏感信息等，检查系统是否被入侵过（存在入侵痕迹）等。

表17 渗透测试检查结果统计表

渗透测试	进行渗透测试的系统数量： 其中，可以成功控制的系统数量：

表18 信息系统渗透测试登记表

1. 信息系统抽查清单				
序号	系统名称	域名或 IP	主管部门	运维单位
1				
2. 存在高、中风险漏洞的信息系统情况				
序号	系统名称	高、中风险漏洞列举/级别		数量
1				
…				
3. 存在入侵痕迹的信息系统情况				
序号	系统名称	入侵痕迹列举		数量
1				
…				
4. 可获取系统权限的信息系统情况				
序号	系统名称	入侵痕迹列举		数量
1				
…				

4.7.1.2 恶意代码及安全漏洞检测

a）可根据工作实际合理安排年度检测的服务器数量，每 1～2 年对所有服务器进行一次技术检测，重要业务系统和门户网站系统的服务器应作为检测重点；

b）使用病毒木马检测工具，检测服务器是否感染了病毒、木马等恶意代码；

c）使用漏洞扫描等工具检测服务器操作系统、端口、应用、服务及补丁更新情况，检测是否关闭了不必要的端口、应用、服务，是否存在安全漏洞。

表19 恶意代码、安全漏洞检测结果统计表

恶意代码检测结果	①进行病毒木马等恶意代码检测的服务器台数：_____ 其中，存在恶意代码的服务器台数：_____ ②进行病毒木马等恶意代码检测的终端计算机台数：_____ 其中，存在恶意代码的终端计算机台数：_____
安全漏洞检测结果	①进行漏洞扫描的服务器台数：_____ 其中，存在高风险漏洞的服务器台数：_____ ②进行漏洞扫描的终端计算机台数：_____ 其中，存在高风险漏洞的终端计算机台数：_____

表20 服务器恶意代码及安全漏洞检测结果记录表

1. 服务器抽查清单				
序号	服务器名称/编号	用途/承载的业务系统重要性（按等级）	主管部门	运维单位
1				
…				
2. 感染病毒木马等恶意代码的服务器情况				
序号	服务器名称/编号	病毒木马等恶意代码名称		数量
1				
2				
…				
3. 存在高风险漏洞的服务器情况				
序号	服务器名称/编号	主要漏洞列举		数量
1				
…				

表21 终端计算机恶意代码及安全漏洞检测结果记录表

1. 终端计算机抽查清单				
序号	计算机名称/编号	责任人	所属部门	备注
1				
…				
2. 感染病毒木马等恶意代码的终端计算机情况				
序号	计算机名称/编号	病毒木马等恶意代码名称		数量
1				
2				
…				
3. 存在高风险漏洞的终端计算机情况				
序号	服务器名称/编号	主要漏洞列举		数量
1				
…				

4.7.2 网络安全事件情况

a）查看入侵检测、网络防火墙、Web 应用防火墙、数据库审计设备中日志记录，统计得出检测到的攻击数；

b）查阅本年度风险评估及系统安全测评评估报告等相关记录文档，统计出网络安全事件数；

c）查阅年度收到各平台发布的网络安全风险提示数。

表22 网络安全事件检查结果表

网络安全事件情况	①监测到的网络攻击次数： 其中：本单位遭受 DDoS 攻击次数： 系统被嵌入恶意代码次数： ②网络安全事件次数： 其中：服务中断次数： 信息泄露次数： 网页被篡改次数：

4.8 外包服务管理情况检查

4.8.1 要求

a）应建立并严格执行信息技术外包服务安全管理制度；

b）应与信息技术外包服务提供商签订服务合同和网络安全与保密协议，明确网络安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何资产，不得以服务为由强制要求委托方购买、使用指定产品；

c）信息技术现场服务过程中应安排专人陪同，并详细记录服务过程；

d）外包开发的系统、软件上线应用前应进行安全测评，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务；

e）信息系统运维外包不得采用远程在线运维服务方式；

4.8.2 检查方式

文档查验、人员访谈。

4.8.3 检查方法

a）查验相关制度文档，检查是否有外包服务安全管理制度；

b）查验信息技术外包服务合同及网络安全与保密协议，检查网络安全责任是否清晰；

c）查验外包人员现场服务记录，查验记录是否完整（包括服务时间、服务人员、陪同人员、工作内容等信息）；

d）访谈系统管理员和工作人员，查验安全测评报告，检查外包开发的系统、软件上线前是否进行过网络安全测评及其方式；

e）查验外包服务合同及技术方案等文档，检查是否存在远程在线运维服务；如确需采用远程在线服务的，检查是否对安全风险进行了充分评估并采取了书面审批、访问控制、在线监测、日志审计等安全防护措施。

表23 外包服务管理检查结果记录表

外包服务机构 1	机构名称	
	机构性质	□国有单位　□民营企业 □外资企业　□合资企业
	服务内容	□系统集成　□系统运维　□风险评估 □安全检测　□安全加固　□应急支持 □数据存储　□数据分析　□灾难备份 □安全监测　□流量清洗　□其他
外包服务机构 2	机构名称	
	机构性质	□国有单位　□民营企业 □外资企业　□合资企业

	服务内容	□系统集成 □系统运维 □风险评估 □安全检测 □安全加固 □应急支持 □数据存储 □数据分析 □灾难备份 □安全监测 □流量清洗 □其他

5 检查总结整改

5.1 汇总检查结果

检查实施完成后，检查办公室应及时对检查结果进行梳理、汇总，从安全管理、技术防护等方面对检查发现的问题和隐患进行分类整理。

5.2 分析问题隐患

检查办公室应对检查发现的问题和隐患逐项进行研究，深入分析产生的原因。结合年度网络安全形势，对本单位面临的网络安全威胁和风险程度、信息系统抵御网络攻击的能力进行评估。

5.3 研究整改措施

检查办公室在深入分析问题隐患的基础上，研究提出针对性的改进措施建议。本单位网络安全管理部门应根据检查办公室的建议，组织相关单位和人员进行整改，对于不能及时整改的，要制定整改计划和时间表，整改完成后应及时进行再评估。

5.4 编写总结报告

本单位网络安全管理部门应组织检查办公室对检查工作进行全面总结，编写检查报告，使用填报工具填报关键信息基础设施清单、自查检查结果统计表，并按要求及时报送。

6 注意事项

6.1 认真做好总结

要按照年度网络安全检查工作的统一要求，进行全面总结，认真编写检查报告。要如实填写检查情况报告表，避免出现漏项、错项、前后不一致等情况。要根据检查报告内容的敏感程度，确定密级并在首页明确标识。

6.2 加强风险控制

要明确相关工作纪律并严格执行。要识别检查中的安全风险，周密制定应急预案，强化风险控制措施，明确发生重大安全事件时的处置流程，确保被检查信息系统的正常运行。要对技术检测活动的安全风险进行评估，防止引入新的风险，并要求相关人员严格遵守操作规程。应对重要数据和配置进行备份，尽量避开业务高峰期进行技术检测。

需委托外部检测机构进行检测的，要对相关检测机构的安全可靠性及其技术能力、管理水平等严格把关，明确检测机构和检测人员的安全责任。可参考以下条件选取检测机构：①机构安全可控（如事业单位）；②开展网络安全检查或相关工作2年以上；③拥有专业安全检查人员10人以上，全部为机构编制内人员或与机构签订2年以上劳动合同的聘用人员；④拥有与开展安全检查相适应的安全检测设备与检测工具；⑤网络安全与保密管理、项目管理、质量管理、人员管理、教育培训等规章制度健全；⑥参与安全检查的人员无犯罪记录，并与机构签订安全保密协议。

6.3 加强保密管理

要高度重视保密工作，指定专人负责，对检查活动、检查实施人员以及相关文档和数据进行严格管理，确保检查工作中涉及到的敏感信息得到有效控制；对检查人员进行保密培训，确保检查工作中获知的信息不被泄露，检查数据和检查结果不向其他单位透露。

附件

网络安全检查总结报告参考格式

一、报告名称

×××（单位名称）×××年网络安全检查总结报告。

二、检查总结报告组成

检查总结报告包括主报告、检查结果统计表及自评估表三部分。

三、主报告内容要求

（一）网络安全检查工作组织开展情况

概述检查工作组织开展情况、所梳理的关键信息基础设施情况。

（二）关键信息基础设施确定情况

此次检查确定关键信息基础设施的数量、分布、功能等情况。

（三）×××年网络安全主要工作情况

详细描述本单位×××年在网络安全管理、技术防护、应急管理、宣传教育等方面开展的工作情况。

（四）检查发现的主要问题和面临的威胁分析

1. 发现的主要问题和薄弱环节

2. 面临的安全威胁与风险

3. 整体安全状况的基本判断

（五）改进措施与整改效果

1. 改进措施

2. 整改效果

（六）关于加强网络安全工作的意见和建议

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　2016 年 6 月 28 日）

第一条　为加强对移动互联网应用程序（APP）信息服务的管理，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》和《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条　在中华人民共和国境内通过移动互联网应用程序提供信息服务，从事互联网应用商店服务，应当遵守本规定。

本规定所称移动互联网应用程序，是指通过预装、下载等方式获取并运行在移动智能终端上、向用户提供信息服务的应用软件。

本规定所称移动互联网应用程序提供者，是指提供信息服务的移动互联网应用程序所有者或运营者。

本规定所称互联网应用商店，是指通过互联网提供应用软件浏览、搜索、下载或开发工具和产品发布服务的平台。

第三条　国家互联网信息办公室负责全国移动互联网应用程序信息内容的监督管理执法工作。地方互联网信息办公室依据职责负责本行政区域内的移动互联网应用程序信息内容的监督管理执法工作。

第四条　鼓励各级党政机关、企事业单位和各人民团体积极运用移动互联网应用程序，推进政务公开，提供公共服务，促进经济社会发展。

第五条　通过移动互联网应用程序提供信息服务，应当依法取得法律法规规定的相关资质。从事互联网应用商店服务，还应当在业务上线运营三十日内向所在地省、自治区、直辖市互联网信息办公室备案。

第六条　移动互联网应用程序提供者和互联网应用商店服务提供者不得利用移动互联网应用程序从事危害国家安全、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动，不得利用移动互联网应用程序制作、复制、发布、传播法律法规禁止的信息内容。

第七条　移动互联网应用程序提供者应当严格落实信息安全管理责任，依法履行以下义务：

（一）按照“后台实名、前台自愿”的原则，对注册用户进行基于移动电话号码等真实身份信息认证。

（二）建立健全用户信息安全保护机制，收集、使用用户个人信息应当遵循合法、正当、必要的原则，明示收集使用信息的目的、方式和范围，并经用户同意。

（三）建立健全信息内容审核管理机制，对发布违法违规信息内容的，视情采取警示、限制功能、暂停更新、关闭账号等处置措施，保存记录并向有关主管部门报告。

（四）依法保障用户在安装或使用过程中的知情权和选择权，未向用户明示并经用户同意，不得开启收集地理位置、读取通讯录、使用摄像头、启用录音等功能，不得开启与服务无关的功能，不得捆绑安装无关应用程序。

（五）尊重和保护知识产权，不得制作、发布侵犯他人知识产权的应用程序。

（六）记录用户日志信息，并保存六十日。

第八条　互联网应用商店服务提供者应当对应用程序提供者履行以下管理责任：

（一）对应用程序提供者进行真实性、安全性、合法性等审核，建立信用管理制度，并向所在地省、自治区、直辖市互联网信息办公室分类备案。

（二）督促应用程序提供者保护用户信息，完整提供应用程序获取和使用用户信息的说明，并向用户呈现。

（三）督促应用程序提供者发布合法信息内容，建立健全安全审核机制，配备与服务规模相适应的专业人员。

（四）督促应用程序提供者发布合法应用程序，尊重和保护应用程序提供者的知识产权。

对违反前款规定的应用程序提供者，视情采取警示、暂停发布、下架应用程序等措施，保存记录并向有关主管部门报告。

第九条　互联网应用商店服务提供者和移动互联网应用程序提供者应当签订服务协议，明确双方权利义务，共同遵守法律法规和平台公约。

第十条　移动互联网应用程序提供者和互联网应用商店服务提供者应当配合有关部门依法进行的监督检查，自觉接受社会监督，设置便捷的投诉举报入口，及时处理公众投诉举报。

第十一条　本规定自 2016 年 8 月 1 日起施行。

市场监管总局、中央网信办关于开展App安全认证工作的公告

（2019年第11号）

为规范移动互联网应用程序（以下称App）收集、使用用户信息特别是个人信息的行为，加强个人信息安全保护，根据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》，市场监管总局、中央网信办决定开展App安全认证工作。现将有关事项公告如下：

一、App安全认证活动依据《移动互联网应用程序（App）安全认证实施规则》（见附件）开展。

二、从事App安全认证的认证机构为中国网络安全审查技术与认证中心，检测机构由认证机构根据认证业务需要和技术能力确定。

三、认证机构和检测机构应按有关规定，客观、公正地开展认证和检测活动，并对认证和检测结果负责。

四、国家鼓励App运营者自愿通过App安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

附件：移动互联网应用程序（App）安全认证实施规则

市场监管总局

中央网信办

2019年3月13日

附件

编号：CNCA-App-001

移动互联网应用程序（App）安全认证实施规则

2019-03-13发布　　2019-03-15实施

国家认证认可监督管理委员会发布

目 录

1 适用范围

本规则适用于对移动互联网应用程序（以下称“App”）的数据安全认证。

2 认证依据

App安全认证的认证依据为 GB/T 35273《信息安全技术个人信息安全规范》及相关标准、规范。

上述标准原则上应执行国家标准化行政主管部门发布的最新版本。

3 认证模式

App安全认证的认证模式为：技术验证+现场核查+获证后监督。

4 认证程序

4.1 认证申请

4.1.1 申请方

认证申请主体为通过App向用户提供服务的网络运营者（以下简称“App运营者”），且取得市场监督管理部门或有关机构注册登记的法人资格。

App运营者有下列情形之一的，不得申请认证：

（1）违反相关法律法规；

（2）在12个月内发生重大信息安全事件；

（3）所持同类证书在撤销认证影响期内；

（4）认证机构规定的其他情况。

4.1.2 申请单元的确定

原则上按App版本申请认证。同一名称的App，版本号、操作系统平台等不同时，一般应分为不同申请单元，具体由认证机构依据本规则制定的认证实施细则予以规定。

4.1.3 申请方应提交的文件和资料

认证申请方在申请认证时，提交的文档资料应至少包含以下内容：

（1）认证申请书；

（2）法人资格证明材料；

（3）App版本控制说明；

（4）对认证要求符合性的自评价结果及相关证明文档；

（5）对App符合相关安全技术标准的证明文件；

（6）不同发布渠道的版本差异性声明；

（7）其他需要的文件。

4.2 认证受理

认证机构对申请资料进行审核后做出受理决定，并向认证申请方反馈受理决定。

4.3 技术验证

4.3.1 样品获取

认证申请方按照申请书填写的送样方式提交样本。

送样副本应反映所有发布渠道App副本与认证相关的技术特性；不能反映时，还应选送申请单元内其他App副本。

4.3.2 技术验证依据的标准

技术验证的依据为 GB/T 35273《信息安全技术个人信息安全规范》。

认证机构应根据GB/T 35273制定技术验证规范，确定针对标准要求的技术验证内容、方法和评价准则。

4.3.3 技术验证方式

技术验证采用实验室检测和现场核查等方式进行。

4.3.4 技术验证实施

检测机构按照技术验证规范实施技术验证，并按照认证机构有关规定出具技术验证报告。

发现不符合时，检测机构向认证申请方出具不符合报告，并要求限期整改；逾期未完成整改的，中止认证过程。

4.4 现场审核

技术验证通过后，认证机构对App运营者进行现场审核。

4.4.1 现场审核依据的标准

现场审核的依据为 GB/T 35273《信息安全技术个人信息安全规范》。

认证机构应根据GB/T 35273制定现场审核规范，确定针对标准要求的现场审核内容、方法和评价准则。

4.4.2 现场审核实施

认证机构按照现场审核规范实施现场审核,并按认证机构有关规定出具现场审核报告。

发现不符合时，认证机构向认证申请方出具不符合报告，并要求限期整改；逾期未完

成整改的，中止认证过程。

4.5 认证决定

认证机构根据申请资料、技术验证结论和现场审核结论等进行综合评价，做出认证决定。认证决定通过后，由认证机构向认证申请方颁发认证证书，并授权获证App运营者使用规定的认证标志。认证决定不通过的，终止认证。

4.6 对认证决定的申诉

认证申请方如对认证决定结果有异议，可在收到认证结果通知后10个工作日内通过认证机构指定的申诉渠道进行申诉。认证机构自收到申诉之日起，应在5个工作日决定是否予以受理；对于受理的申诉，一般应在30个工作日给出处理结果，并将处理结果书面通知认证申请方。

4.7 获证后监督

获证App运营者应持续进行获证后自评价，并配合认证机构的监督活动。

认证机构应对获证App和App运营者实施持续监督，监督方式包括日常监督和专项监督。

4.7.1 获证后自评价

获证 App 运营者应对获证 App 持续符合认证要求的情况进行自评价。当出现如下情形时，获证 App 运营者应向认证机构提交自评价报告：

（1）获证App的分发渠道发生变化；

（2）认证标志使用情况发生变化；

（3）获证App发生变更，以及所引起的收集、处理和使用个人信息的目的、类型、方式发生变化；

（4）获证App运营者对所收集个人信息的共享、转让、公开披露的对象、方式和目的发生变化；

（5）获证App运营者收到获证App个人信息保护相关的投诉举报。

4.7.2 日常监督

认证机构应对获证 App 和 App 运营者持续实施日常监督，日常监督的内容至少包括以下方面：

（1）获证App一致性检查；

（2）获证App的更新情况；

（3）认证证书和认证标志的使用情况；

（4）企业开展自评价的情况；

（5）获证App被网民举报投诉和社会媒体曝光情况；

（6）其他影响获证App在个人信息收集、处理和使用方面持续符合认证要求的情况。

认证机构应定期对日常监督情况进行评价，形成日常监督报告。

4.7.3 专项监督

当出现如下情形，认证机构应启动专项监督：

（1）网民举报投诉、媒体曝光、行业通报等涉及获证App存在个人信息安全方面的问题，并经查实获证App运营者负有责任时；

（2）获证App运营者因组织架构、服务模式等发生重大变更，或发生破产并购等可能影响App认证特性符合性时；

（3）认证机构根据日常监督结果，对获证App与本规则中规定的标准要求的符合性提出具体质疑时。

专项监督应对上述情形进行深入调查，并对获证 App 持续符合性全面审核，必要时还可进行技术验证。

认证机构可采取事先不通知的方式对获证 App 运营者实施专项监督。

4.7.4 监督结果的处理

获证后监督中发现不符合时，认证机构应要求获证App运营者在限期内进行整改，并对整改结果进行验证。未在规定期限内完成整改或整改结果未通过验证的，按照6.3规定处置。

5 认证时限

认证时限是指自作出受理决定之日起至作出认证决定所实际发生的工作日，一般为90个工作日（不包含整改时间）。

6 认证证书

6.1 证书的保持

认证机构应对认证证书的有效期做出规定，超过有效期的认证证书自行失效。当认证规则要求（如标准）发生变化时，应在认证机构确定的转换期限内完成换证。

6.2 证书的变更

6.2.1 变更申请与通知

出现下列情况之一时，获证 App 运营者应向认证机构提出变更申请：

（1）获证App名称、版本发生变更；

（2）认证范围扩大或缩小；

（3）获证App运营者名称、注册地址发生变更；

（4）认证机构规定的其它事项发生变更时。

6.2.2 变更评价和批准

认证机构根据变更的内容，对提供的资料进行评价，确定是否可以批准变更。如需重新技术验证和现场审核，应在技术验证和/或现场审核通过后方能批准变更。

6.3 认证的暂停、撤销和注销

6.3.1 暂停认证

有下列情形之一的，认证机构应暂停认证，并予以公布：

（1）国家有关主管部门发现获证App存在安全问题；

（2）在监督中发现获证App不能持续符合认证要求；

（3）获证App运营者在App发生重大变更后，未及时向认证机构报告变更情况；

（4）获证App运营者违规使用认证证书、认证标志；

（5）认证标准或认证规则发生变化，获证App运营者未按认证机构规定完成过渡转换；

（6）获证App运营者主动申请暂停认证；

（7）其他依法应当暂停的情形。

暂停期限一般为180天。暂停期限内，获证App运营者可提出恢复认证的申请，认证机构经审核、批准后，方可使用该证书。在暂停认证期间，获证App运营者不得继续使用证书和认证标志。

6.3.2 撤销认证

有下列情形之一的，认证机构应撤销认证，并予以公布：

（1）获证App运营者存在个人信息安全有关的违规违法行为；

（2）暂停认证期间，获证App运营者未采取有效整改措施；

（3）发现获证App运营者在认证过程中存在欺骗、隐瞒、违反承诺等不当行为，影响认证有效性；

（4）获证App运营者拒绝接受获证后监督；

（5）超过暂停期限；

（6）其他依法应当撤销的情形。

撤销认证后，获证App运营者应交回认证证书，停止使用认证标志。

6.3.3 注销认证

有下列情形之一的，认证机构应注销认证，并予以公布：

（1）获证App不再向用户提供服务；

（2）获证App运营者申请注销；

（3）其他依法应当注销的情形。

注销认证后，获证App运营者应交回认证证书，停止使用认证标志。

7 认证证书和认证标志的使用和管理

7.1 认证证书的使用和管理

在认证证书有效期内，获证 App 运营者可将证书在网站、工作场所和宣传资料中展示，但不应进行误导性宣传。

7.2 认证标志及其使用和管理

7.2.1 认证标志的式样

认证标志的式样由基本图案、认证机构识别信息组成。

A B C D

“ABCD”代表认证机构识别信息。

7.2.2 认证标志的使用和管理

认证机构应规定认证标志的使用和管理。

获证App运营者应按照认证机构的规定使用和管理认证标志，不得进行误导性宣传。

8 认证责任

认证机构应对其做出的认证结论负责。

检测机构应对技术验证结果和技术验证报告负责。

认证机构及其所委派的审核员应对现场审核结论负责。

认证申请方（获证App运营者）应对其所提交的申请资料及样品的真实性、合法性负责，

并对获证App持续符合认证要求负主体责任。

认证不能免除获证 App 运营者对获证 App 承担的法律责任。

市场监管总局等部门关于印发2019网络市场监管专项行动（网剑行动）方案的通知

（国市监网监〔2019〕118号）

各省、自治区、直辖市及新疆建设兵团市场监管局（厅、委）、发展改革委、通信管理局、公安厅（局）、商务厅（局）、网信办、邮政管理局、海关总局广东分署、各直属海关：

为深入贯彻党的十九大和十九届二中、三中全会精神，充分发挥网络市场监管部际联席会议各成员单位职能优势，贯彻落实《电子商务法》，着力规范电子商务主体资格，严厉打击网络市场突出问题，落实电子商务经营者责任，维护良好网络市场秩序，网络市场监管部际联席会议各成员单位决定于6-11月联合开展2019网络市场监管专项行动（网剑行动）。现将《2019网络市场监管专项行动（网剑行动）方案》印发给你们，请结合实际，认真贯彻执行。

市场监管总局

发展改革委

工业和信息化部

公安部

商务部

海关总署

网信办

邮政局

2019年6月17日

2019网络市场监管专项行动（网剑行动）方案

为深入贯彻党的十九大和十九届二中、三中全会精神，以落实《电子商务法》为统领，规范网络经营行为，净化网络市场交易环境，维护良好网络市场秩序，网络市场监管部际联席会议各成员单位决定于6-11月联合开展2019网络市场监管专项行动（网剑行动）。具体方案如下：

一、总体目标

充分发挥网络市场监管部际联席会议作用，严格贯彻落实《电子商务法》有关规定，严厉打击网络市场突出问题，营造公平竞争的市场秩序。坚持依法依规监管、审慎监管、智慧监管、综合监管和协同监管，强化信用约束，规范电子商务行为，净化交易环境，保护消费者和经营者合法权益，提升网络商品和服务质量，促进电子商务持续健康发展。

二、重点任务

（一）着力规范电子商务主体资格，营造良好准入环境。依法查处电子商务经营者违反《电子商务法》第十五条规定的信息公示义务的行为。监督电子商务经营者依法办理市场主体登记，规范电子商务主体资格，加强对社交电商、跨境电商经营者的规范引导。督促电子商务平台经营者按照《电子商务法》等法律法规要求登记备案，对进入平台的经营者真实信息进行核验、登记，建立登记档案，监督电子商务经营者做好亮照、亮证、亮标工作。督促邮政企业、快递企业加强对电子商务企业协议客户经营范围的审查。规范电子商务经营主体，集中整治非法主体互联网应用（网站、APP 等）。（市场监管总局、工业和信息化部、公安部、海关总署、邮政局按职责分工协作）

（二）严厉打击网上销售假冒伪劣产品、不安全食品及假药劣药，营造放心消费环境。以食品（含保健食品）、药品、电子产品、汽车配件、家具家装、家庭日用品、儿童用品、服装鞋帽以及劳动防护安全帽等社会反映集中、关系健康安全的消费品为重点，加强监管执法和刑事司法，以大要案为突破口，组织开展集中打击，坚决守住人民生命健康和安全的底线。坚持线上线下治理相结合，加强流通销售餐饮环节食品等商品抽查，加强网络餐饮服务食品安全监管，加强风险监测，净化生产源头，依法查处利用互联网销售假冒伪劣商品违法犯罪活动。依法依规处置互联网侵权假冒有害信息。（市场监管总局、公安部、海关总署、邮政局按职责分工协作）

（三）严厉打击不正当竞争行为，营造公平竞争的市场环境。按照《反不正当竞争法》《电子商务法》等相关规定，严厉打击网络虚假宣传、刷单炒信、违规促销、违法搭售等行为。严肃查处违规推销宣传婴幼儿配方食品的行为。严厉打击通过组织非法寄递空包裹等方式，帮助其他经营者进行刷单炒信等违法行为。督促电子商务平台经营者进一步加强对刷单炒信行为的监测监控，完善商品（服务）信用评价体系，配合执法工作开展。依法查处电子商务平台经营者限制平台内经营者参与其他第三方电子商务平台经营活动等行

为。（市场监管总局、发展改革委、商务部、邮政局按职责分工协作）

（四）深入开展互联网广告整治工作，营造良好广告市场环境。以社会影响大、覆盖面广的门户网站、搜索引擎、电子商务平台为重点，突出移动客户端和新媒体账户等互联网媒介，针对医疗、药品、保健食品、房地产、金融投资理财等关系人民群众身体健康和财产安全的虚假违法广告，加大案件查处力度，查办一批大案要案。（市场监管总局、工业和信息化部、公安部、网信办按职责分工协作）

（五）依法打击其他各类网络交易违法行为，有效净化网络市场环境。落实《电子商务法》《网络安全法》《消费者权益保护法》《价格法》《网络购买商品七日无理由退货暂行办法》等相关规定，畅通消费投诉举报渠道，保护消费者知情权和选择权，加大对不正当价格行为、不公平格式条款、不依法履行七日无理由退货义务等侵害消费者权益行为的打击力度。全方位多渠道加大个人信息保护力度，规范涉及个人信息的合同格式条款；严肃查处未经同意收集、使用、过度收集或泄露、非法出售、非法向他人提供个人信息行为，依法查处不履行个人信息保护义务、为网络违法犯罪提供支持帮助的网络平台；严厉打击侵犯公民个人信息犯罪，切实防范大数据技术对个人信息的滥用。依法严厉打击网络交易平台为违法出售、购买、利用野生动物及其制品或者禁止使用的猎捕工具提供交易服务的行为。密切协作配合，加强对手机 APP 端（网络交易平台、网络订餐平台、在线旅游平台、社交电商、跨境电商以及其他网络市场新模式新业态）违法犯罪行为的研判、监管和打击查处。加大对网络销售单用途商业预付卡违规行为的查处力度。严格海外代购行为监管，加大对跨境电商进出口环节整治力度。加强对网络销售禁止交易商品的监测监管工作，不断净化网络市场环境。（市场监管总局、工业和信息化部、公安部、商务部、海关总署、网信办、邮政局按职责分工协作）

（六）强化网络交易信息监测和产品质量抽查，营造良好消费环境。不断强化监管技术应用，探索应用网络交易信息监测的新方式，完善监测监管流程，有效发现网络交易违法线索。重点关注网络集中促销期、节假日等重要时间节点，开展网络市场定向监测和产品质量抽检，及时发现风险，发挥部门失信联合惩戒作用，实施全网警示。（市场监管总局、发展改革委、工业和信息化部、公安部、商务部、海关总署、网信办、邮政局按职责分工协作）

（七）落实电子商务经营者责任，营造诚信守法经营环境。督促电子商务经营者特别

是平台经营者履行法定责任和义务。监督电子商务经营者履行消费者权益、知识产权、个人信息保护等方面的义务，依法承担产品和服务质量责任，严格落实网络销售商品修理更换退货责任。指导和督促电子商务平台经营者加强对平台内经营者的资格审查、主体信息公示，落实知识产权保护“通知-删除”义务、显著标明竞价排名商品（服务）为“广告”义务；指导和督促网络餐饮服务平台加强分支机构、代理商、合作商管理，主动向监管部门报送平台入网餐饮服务提供者数据和平台分支机构、代理商、合作商等信息，加强餐食配送过程管理，逐步推动外卖餐食封签，确保食品配送过程不受污染。指导和督促配送、邮政、快递等企业完善实名制，拒绝接收、寄递侵权假冒商品，为执法部门核查违法犯罪线索提供支持。（市场监管总局、发展改革委、工业和信息化部、公安部、商务部、海关总署、网信办、邮政局按职责分工协作）

三、有关工作要求

（一）加强组织保障，扎实部署推进。各地各部门要落实属地监管责任，立足本地实际，认真做好整体部署，制定切实可行的具体实施方案，务求取得实效。

（二）提升监管效能，创新网络市场监管方式。各地要充分发挥网络市场监管联席会议作用，形成监管合力。综合运用行政指导、行政约谈、行政处罚等手段，督促电子商务经营者、特别是平台经营者履行法定责任和义务。扎实推进“双随机、一公开”监管。通过“信用中国”网站和国家企业信用信息公示系统，及时公示电子商务经营者的基础信息和各部门履职中形成的行政许可、行政处罚、抽查检查结果等监管执法信息，进一步加强部门间协同监管和联合惩戒。

（三）增强法律意识，加大《电子商务法》宣传力度。各地各部门要通过多种形式开展广泛宣传，组织开展电子商务经营者座谈、约谈，发布消费预警、提示警示和违法典型案例，营造电子商务参与各方学法、知法、守法、懂法、用法的良好氛围，多措并举做好《电子商务法》宣贯工作。

各地各部门要突出工作重点，强化源头治理，科学安排工作进度，于 12 月 12 日前将本系统专项行动总结报告、专项行动情况统计表、典型案例（5 件以上，附行政处罚决定书）、联合执法相关材料分别报各上级主管部门，并抄送同级市场监管部门。如遇重大情况，请及时报告当地党委政府和各上级主管部门。

附件：2019 网络市场监管专项行动情况统计表（略）

中央网络安全和信息化委员会办公室关于做好个人信息保护利用大数据支撑联防联控工作的通知

各省、自治区、直辖市网络安全和信息化委员会，中央和国家机关有关部委：

为做好新型冠状病毒感染肺炎疫情联防联控中的个人信息保护，积极利用包括个人信息在内的大数据支撑联防联控工作，经中央网络安全和信息化委员会同意，现将有关事项通知如下：

1.各地方各部门要高度重视个人信息保护工作，除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。法律、行政法规另有规定的，按其规定执行。

2.收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视。

3.为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。

4.收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

5.鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持。

6.任何组织和个人发现违规违法收集、使用、公开个人信息的行为，可以及时向网信、公安部门举报。网信部门要依据《中华人民共和国网络安全法》和相关规定，及时处置违规违法收集、使用、公开个人信息的行为，以及造成个人信息大量泄露的事件；涉及犯罪的公安机关要依法严厉打击。

中央网络安全和信息化委员会办公室

2020 年 2 月 4 日

中央网信办、工业和信息化部、公安部、市场监管总局关于开展App违法违规收集使用个人信息专项治理的公告

近年来，移动互联网应用程序（App）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。同时，App强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。落实《网络安全法》《消费者权益保护法》的要求，为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和信息化部、公安部、市场监管总局决定，自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理。现将有关事项公告如下：

一、App运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则， 并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权,不得违反法律法规和与用户的约定收集使用个人信息。倡导App运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。

三、有关主管部门加强对违法违规收集使用个人信息行为的监管和处罚，对强制、过度收集个人信息，未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，按照《网络安全法》《消费者权益保护法》等依法予以处罚，包括责令App运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。

四、公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。

五、开展App个人信息安全认证，鼓励App运营者自愿通过App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

特此公告。

中央网络安全和信息化委员会办公室

工业和信息化部

公安部

市场监管总局

2019 年 1 月 23 日

工业和信息化部关于开展APP侵害用户权益专项整治工作的通知

（工信部信管函〔2019〕337号）

各省、自治区、直辖市通信管理局，中国信息通信研究院、中国互联网协会，各相关单位：

当前，APP违规收集个人信息、过度索权、频繁骚扰、侵害用户权益等问题突出，群众反映强烈，社会关注度高。结合2019年信息通信行业行风建设暨纠风工作安排，我部决定组织开展APP侵害用户权益专项整治行动工作。有关事项通知如下：

一、整治内容

依据《网络安全法》、《电信条例》、《规范互联网信息服务市场秩序若干规定》（工业和信息化部令第20号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号）和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等法律法规和规范性文件要求，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，重点对以下四个方面8类问题开展规范整治工作。

（一）违规收集用户个人信息方面

1.“私自收集个人信息”。即APP未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。

2.“超范围收集个人信息”。即APP收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。

（二）违规使用用户个人信息方面

3.“私自共享给第三方”。即APP未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

4.“强制用户使用定向推送功能”。即APP未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。

（三）不合理索取用户权限方面

5.“不给权限不让用”。即APP安装和运行时，向用户索取与当前服务场景无关的权

限，用户拒绝授权后，应用退出或关闭。

6.“频繁申请权限”。即APP在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。

7.“过度索取权限”。即APP在用户未使用相关功能或服务时，提前申请开启通讯录、定位、短信、录音、相机等权限，或超出其业务功能或服务外，申请通讯录、定位、短信、录音、相机等权限。

（四）为用户账号注销设置障碍方面

8.“账号注销难”。即APP未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

二、整治对象

本次专项整治工作主要面向两类对象：一是APP服务提供者，主要检查是否存在前述8类问题；二是APP分发服务提供者，含应用商店和基础电信企业营业厅等承担APP分发功能的各类企业，主要检查是否落实《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407号）等有关要求。

三、工作安排

专项整治工作时间为通知印发之日至2019年12月20日。分三个阶段实施：

（一）企业自查自纠阶段（通知印发之日起至11月10日）。APP服务提供者对照前述8类问题认真开展自查，发现问题及时整改；APP分发服务提供者组织对所分发APP进行全面检查，对存在问题的违规应用软件予以督促整改，拒不改正的应组织予以下架处理。

（二）监督抽查阶段（2019年11月11日至11月30日）。我部将组织第三方检测机构对APP进行技术检测和检查，重点抽测与群众生活密切相关、下载使用量较大的APP产品和分发平台。对群众反映强烈、难以接受、认为不合理的APP，我部将组织电信用户委员会、中国互联网协会以及相关媒体机构开展用户和专家评议。各省、自治区、直辖市通信管理局可根据本地实际情况开展检查工作，并将结果报部（信息通信管理局）。

（三）结果处置阶段（2019年12月1日至12月20日）。我部将对存在问题的APP统一进行通报，依法依规予以处理，具体措施包括责令整改、向社会公告、组织APP下架、停止APP接入服务，以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等。

四、工作要求

（一）切实提高思想认识。各单位要坚决贯彻落实以人民为中心的发展思想，切实提高政治站位，高度重视本次专项整治工作，精心组织、周密部署，细化整治措施，着力解决群众最关心最直接最现实的利益问题，务求取得实效。

（二）畅通用户投诉渠道。专项整治工作期间，各企业应畅通用户投诉渠道，完善投诉处理服务机制和流程。中国互联网协会应通过互联网信息服务投诉平台（https://ts.isc.org.cn/）或 12321 举报中心接受群众投诉，及时汇总处理用户反映的相关问题。

（三）巩固建立长效机制。APP 用户量大、影响面广、耦合性强，规范管理工作涉及主体多、链条长，需要企业自律、社会监督和政府监管的协同共治。各单位要以此次专项整治工作为契机，不断总结经验、分析原因、举一反三、巩固成效，为后续规范行业管理奠定基础。

特此通知。

（联系电话：010-66011239/68206119）

工业和信息化部

2019 年 10 月 31 日

国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅关于印发《App 违法违规收集使用个人信息行为认定方法》的通知

（国信办秘字〔2019〕191 号）

各省、自治区、直辖市及新疆生产建设兵团网信办、通信管理局、公安厅（局）、市场监管局（厅、委）：

根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为认定 App 违法违规收集使用个人信息行为提供参考，落实《网络安全法》等法律法规，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App 违法违规收集使用个人信息行为认定方法》。现印发你们，请结合监管和执法工作实际参考执行。

国家互联网信息办公室秘书局

工业和信息化部办公厅

公安部办公厅

市场监管总局办公厅

2019 年 11 月 28 日

App 违法违规收集使用个人信息行为认定方法

根据《关于开展 App 违法违规收集使用个人信息专项治理的公告》，为监督管理部门认定 App 违法违规收集使用个人信息行为提供参考，为 App 运营者自查自纠和网民社会监督提供指引，落实《网络安全法》等法律法规，制定本方法。

一、以下行为可被认定为“未公开收集使用规则”

1.在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2.在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3.隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；

4.隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未

提供简体中文版等。

二、以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1.未逐一列出App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等；

2.收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3.在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4.有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

三、以下行为可被认定为“未经用户同意收集使用个人信息”

1.征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2.用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3.实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4.以默认选择同意隐私政策等非明示方式征求用户同意；

5.未经用户同意更改其设置的可收集个人信息权限状态，如App更新时自动将用户设置的权限恢复到默认状态；

6.利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7.以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8.未向用户提供撤回同意收集个人信息的途径、方式；

9.违反其所声明的收集使用规则，收集使用个人信息。

四、以下行为可被认定为“违反必要原则，收集与其提供的服务无关的个人信息”

1.收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关；

2.因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能；

3.App新增业务功能申请收集的个人信息超出用户原有同意范围，若用户不同意，则拒绝提供原有业务功能，新增业务功能取代原有业务功能的除外；

4.收集个人信息的频度等超出业务功能实际需要；

5.仅以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，强制要求用户同意收集个人信息；

6.要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用。

五、以下行为可被认定为“未经同意向他人提供个人信息”

1.既未经用户同意，也未做匿名化处理，App 客户端直接向第三方提供个人信息，包括通过客户端嵌入的第三方代码、插件等方式向第三方提供个人信息；

2.既未经用户同意，也未做匿名化处理，数据传输至 App 后台服务器后，向第三方提供其收集的个人信息；

3.App 接入第三方应用，未经用户同意，向第三方应用提供个人信息。

六、以下行为可被认定为“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”

1.未提供有效的更正、删除个人信息及注销用户账号功能；

2.为更正、删除个人信息或注销用户账号设置不必要或不合理条件；

3.虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理；

4.更正、删除个人信息或注销用户账号等用户操作已执行完毕，但 App 后台并未完成的；

5.未建立并公布个人信息安全投诉、举报渠道，或未在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）受理并处理的。

上海市互联网应用商店备案须知

一、设立依据

《移动互联网应用程序信息服务管理规定》第二条 在中华人民共和国境内通过移动互联网应用程序提供信息服务，从事互联网应用商店服务，应当遵守本规定。本规定所称互联网应用商店，是指通过互联网提供应用软件浏览、搜索、下载或开发工具和产品发布服务的平台。

《移动互联网应用程序信息服务管理规定》第五条 从事互联网应用商店服务，还应当在业务上线运营三十日内向所在地省、自治区、直辖市互联网信息办公室备案。

备案工作按照应用商店 ICP 备案地或许可证申领地划分。

二、备案材料

（一）材料目录

1、互联网应用商店备案表

2、主体身份证明

主体为自然人的，提供负责人身份证明复印件；主体为法人的，提供单位有效证件（企业营业执照、事业单位法人证等）复印件和法定代表人身份证明复印件。

3、域名证书复印件

4、互联网应用商店与移动互联网应用程序提供者签订的服务协议范本

5、移动应用程序提供者安全承诺书范本（内容可包含在服务协议中）

6、互联网应用商店平台公约范本（内容可包含在服务协议中）

（二）形式要求

1、上述材料均需加盖单位公章（主体为自然人的，则由负责人签字）。

2、原则上每家单位汇总形成一套材料（无须装订成册），一式两套，报送至上海市网信办。

3、上述材料的电子版（无须盖章）随纸质版一并报送。

（三）接收方式

邮寄地址：上海市徐汇区宛平路 315 号 1307 室

邮政编码：200030

收件人：上海市互联网信息办公室政策法规处

咨询电话：64743030 转 2506

电子邮件：wxbfgc@shanghai.gov.cn

三、备案费用

此项备案无任何收费。

四、变更程序

上海市互联网应用商店备案事项发生变更的，应当及时向上海市互联网信息办公室重新办理备案。已备案的应用商店在永久停止服务后 30 日内向上海市互联网信息办公室申请注销备案。

五、备案结果

有关备案结果，上海市网信办将在备案材料提交后 20 个工作日内以书面形式反馈各申请对象。

上海市互联网信息办公室

2017 年 2 月

国家互联网信息办公室关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知

为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，促进网络信息依法有序自由流动，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，我办会同相关部门起草了《个人信息和重要数据出境安全评估办法（征求意见稿）》，现向社会公开征求意见。有关单位和各界人士可以在2017年5月11日前，通过以下方式提出意见：

一、通过信函方式将意见寄至：北京市东城区朝阳门内大街225号国家互联网信息办公室网络安全协调局，邮编：100010，并在信封上注明“征求意见”。

二、通过电子邮件方式发送至：security@cac.gov.cn。

附件：个人信息和重要数据出境安全评估办法（征求意见稿）

国家互联网信息办公室　2017年4月11日

个人信息和重要数据出境安全评估办法（征求意见稿）

第一条 为保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法利益，根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 网络运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据，应当在境内存储。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。

第三条 数据出境安全评估应遵循公正、客观、有效的原则，保障个人信息和重要数据安全，促进网络信息依法有序自由流动。

第四条 个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

第五条 国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估。

第六条 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。

第七条 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。

第八条 数据出境安全评估应重点评估以下内容：

（一）数据出境的必要性；

（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；

（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；

（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；

（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；

（七）其他需要评估的重要事项。

第九条 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：

（一）含有或累计含有 50 万人以上的个人信息；

（二）数据量超过 1000GB；

（三）包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；

（四）包含关键信息基础设施的系统漏洞、安全防护等网络安全信息；

（五）关键信息基础设施运营者向境外提供个人信息和重要数据；

（六）其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

行业主管或监管部门不明确的，由国家网信部门组织评估。

第十条 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。

第十一条 存在以下情况之一的，数据不得出境：

（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；

（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；

（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。

第十二条 网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。

当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。

第十三条 对违反相关法律法规和本办法向境外提供数据的行为，任何个人和组织有权向国家网信部门、公安部门等有关部门举报。

第十四条 违反本办法规定的，依照有关法律法规进行处罚。

第十五条 我国政府与其他国家、地区签署的关于数据出境的协议，按照协议的规定执行。

涉及国家秘密信息的按照相关规定执行。

第十六条 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。

第十七条 本办法下列用语的含义：

网络运营者，是指网络的所有者、管理者和网络服务提供者。

数据出境，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。

个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。

第十八条 本办法自 2017 年 月 日起实施。

信息安全技术 公共及商用服务信息系统个人信息保护指南

（GB/Z 28828-2012 国家质量监督检验检疫总局、国家标准化管理委员会 2012 年 11 月 5 日批准发布 2013 年 2 月 1 日起实施）

随着信息技术的广泛应用和互联网的不断普及，个人信息在社会、经济活动中的地位日益凸显，滥用个人信息的现象随之出现，给社会秩序和个人切身利益带来了危害。为促进个人信息的合理利用，指导和规范利用信息系统处理个人信息的活动，制定本指导性技术文件。

1 范围

本指导性技术文件规范了全部或部分通过信息系统进行个人信息处理的过程，为信息系统中个人信息处理不同阶段的个人信息保护提供指导。

本指导性技术文件适用于指导除政府机关等行使公共管理职责的机构以外的各类组织和机构，如电信、金融、医疗等领域的服务机构，开展信息系统中的个人信息保护工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T20269-2006 信息安全技术信息系统安全管理要求

GB/Z20986-2007 信息安全技术信息安全事件分类分级指南

3 术语和定义

GB/T20269-2006 和 GB/Z20986-2007 中界定的以及下列术语和定义适用于本技术性指导文件。

3.1 信息系统 informationsystem

即计算机信息系统，由计算机（含移动通信终端）及其相关的和配套的设备、设施（含网络）构成，能够按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索

等处理。

3.2 个人信息 personalinformation

可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。个人信息可以分为个人敏感信息和个人一般信息。

3.3 个人信息主体 subjectofpersonalinformation

个人信息指向的自然人。

3.4 个人信息管理者 administratorofpersonalinformation

决定个人信息处理的目的和方式，实际控制个人信息并利用信息系统处理个人信息的组织和机构。

3.5 个人信息获得者 receiverofpersonalinformation

从信息系统获取个人信息的个人、组织和机构，依据个人信息主体的意愿对获得的个人信息进行处理。

3.6 第三方测评机构 thirdpartytestingandevaluationagency

独立于个人信息管理者的专业测评机构。

3.7 个人敏感信息 personalsensitiveinformation

一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

3.8 个人一般信息 personalgeneralinformation

除个人敏感信息以外的个人信息。

3.9 个人信息处理 personalinformationhandling

处置个人信息的行为，包括收集、加工、转移、删除。

3.10 默许同意 tacitconsent

在个人信息主体无明确反对的情况下，认为个人信息主体同意。

3.11 明示同意 expressedconsent

个人信息主体明确授权同意，并保留证据。

4 个人信息保护概述

4.1 角色和职责

4.1.1 综述

信息系统个人信息保护实施过程中涉及的角色主要有个人信息主体、个人信息管理者、个人信息获得者和独立测评机构，其职责见 4.1.2 至 4.1.5。

4.1.2 个人信息主体

在提供个人信息前，要主动了解个人信息管理者收集的目的、用途等信息，按照个人意愿提供个人信息；发现个人信息出现泄漏、丢失、篡改后，向个人信息管理者投诉或提出质询，或向个人信息保护管理部门发起申诉。

4.1.3 个人信息管理者

负责依照国家法律、法规和本指导性技术文件，规划、设计和建立信息系统个人信息处理流程；制定个人信息管理制度、落实个人信息管理责任；指定专门机构或人员负责机构内部的个人信息保护工作，接受个人信息主体的投诉与质询；制定个人信息保护的教育培训计划并组织落实；建立个人信息保护的内控机制，并定期对信息系统个人信息的安全状况、保护制度及措施的落实情况进行自查或委托独立测评机构进行测评。

管控信息系统个人信息处理过程中的风险，对个人信息处理过程中可能出现的泄露、丢失、损坏、篡改、不当使用等事件制定预案；发现个人信息遭到泄漏、丢失、篡改后，及时采取应对措施，防止事件影响进一步扩大，并及时告知受影响的个人信息主体；发生重大事件的，及时向个人信息保护管理部门通报。

接受个人信息保护管理部门对个人信息保护状况的检查、监督和指导，积极参与和配合第三方测评机构对信息系统个人信息保护状况的测评。

4.1.4 个人信息获得者

当个人信息的获取是出于对方委托加工等目的，个人信息获得者要依照本指导性技术文件和委托合同，对个人信息进行加工，并在完成加工任务后，立即删除相关个人信息。

4.1.5 第三方测评机构

从维护公众利益角度出发、根据个人信息保护管理部门和行业协会的授权、或受个人信息管理者的委托，依据相关国家法律、法规和本指导性技术文件，对信息系统进行测试和评估，获取个人信息保护状况，作为个人信息管理者评价、监督和指导个人信息保护的依据。

4.2 基本原则

个人信息管理者在使用信息系统对个人信息进行处理时，宜遵循以下基本原则：

a）目的明确原则--处理个人信息具有特定、明确、合理的目的，不扩大使用范围，不在个人信息主体不知情的情况下改变处理个人信息的目的。

b）最少够用原则--只处理与处理目的有关的最少信息，达到处理目的后，在最短时间内删除个人信息。

c）公开告知原则--对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。

d）个人同意原则--处理个人信息前要征得个人信息主体的同意。

e）质量保证原则--保证处理过程中的个人信息保密、完整、可用，并处于最新状态。

f）安全保障原则--采取适当的、与个人信息遭受损害的可能性和严重性相适应的管理措施和技术手段，保护个人信息安全，防止未经个人信息管理者授权的检索、披露及丢失、泄露、损毁和篡改个人信息。

g）诚信履行原则--按照收集时的承诺，或基于法定事由处理个人信息，在达到既定目的后不再继续处理个人信息。

h）责任明确原则--明确个人信息处理过程中的责任，采取相应的措施落实相关责任，并对个人信息处理过程进行记录以便于追溯。

5 个人信息保护

5.1 概述

信息系统中个人信息的处理过程可分为收集、加工、转移、删除 4 个主要环节。对个人信息的保护贯穿于 4 个环节中：

a）收集指对个人信息进行获取并记录。

b）加工指对个人信息进行的操作，如录入、存储、修改、标注、比对、挖掘、屏蔽等。

c）转移指将个人信息提供给个人信息获得者的行为，如向公众公开、向特定群体披露、由于委托他人加工而将个人信息复制到其他信息系统等。

d）删除指使个人信息在信息系统中不再可用。

5.2 收集阶段

5.2.1 要具有特定、明确、合法的目的。

5.2.2 收集前要采用个人信息主体易知悉的方式，向个人信息主体明确告知和警示如下事项：

a）处理个人信息的目的；

b）个人信息的收集方式和手段、收集的具体内容和留存时限；

c）个人信息的使用范围，包括披露或向其他组织和机构提供其个人信息的范围；

d）个人信息的保护措施；

e）个人信息管理者的名称、地址、联系方式等相关信息；

f）个人信息主体提供个人信息后可能存在的风险；

g）个人信息主体不提供个人信息可能出现的后果；

h）个人信息主体的投诉渠道；

i）如需将个人信息转移或委托于其他组织和机构，要向个人信息主体明确告知包括但不限于以下信息：转移或委托的目的、转移或委托个人信息的具体内容和使用范围、接受委托的个人信息获得者的名称、地址、联系方式等。

5.2.3 处理个人信息前要征得个人信息主体的同意，包括默许同意或明示同意。收集个人一般信息时，可认为个人信息主体默许同意，如果个人信息主体明确反对，要停止收集或删除个人信息；收集个人敏感信息时，要得到个人信息主体的明示同意。

5.2.4 只收集能够达到已告知目的的最少信息。

5.2.5 要采用已告知的手段和方式直接向个人信息主体收集，不采取隐蔽手段或以间接方式收集个人信息。

5.2.6 持续收集个人信息时提供相关功能，允许个人信息主体配置、调整、关闭个人信息收集功能。

5.2.7 不直接向未满 16 周岁的未成年人等限制民事行为能力或无行为能力人收集个人敏感信息，确需收集其个人敏感信息的，要征得其法定监护人的明示同意。

5.3 加工阶段

5.3.1 不违背收集阶段已告知的使用目的，或超出告知范围对个人信息进行加工。

5.3.2 采用已告知的方法和手段。

5.3.3 保证加工过程中个人信息不被任何与处理目的无关的个人、组织和机构获知。

5.3.4 未经个人信息主体明示同意，不向其他个人、组织和机构披露其处理的个人信息。

5.3.5 保证加工过程中信息系统持续稳定运行，个人信息处于完整、可用状态，且保持最新。

5.3.6 个人信息主体发现其个人信息存在缺陷并要求修改时，个人信息管理者要根据个人信息主体的要求进行查验核对，在保证个人信息完整性的前提下，修改或补充相关信息。

5.3.7 详细记录对个人信息的状态，个人信息主体要求对其个人信息进行查询时，个人信息管理者要如实并免费告知是否拥有其个人信息、拥有其个人信息的内容、个人信息的加工状态等内容，除非告知成本或者请求频率超出合理的范围。

5.4 转移阶段

5.4.1 不违背收集阶段告知的转移目的，或超出告知的转移范围转移个人信息。

5.4.2 向其他组织和机构转移个人信息前，评估其是否能够按照本指导性技术文件的要求处理个人信息，并通过合同明确该组织和机构的个人信息保护责任。

5.4.3 保证转移过程中，个人信息不被个人信息获得者之外的任何个人、组织和机构所获知。

5.4.4 保证转移前后，个人信息的完整性和可用性，且保持最新。

5.4.5 未经个人信息主体的明示同意，或法律法规明确规定，或未经主管部门同意，个人信息管理者不得将个人信息转移给境外个人信息获得者，包括位于境外的个人或境外注册的组织和机构。

5.5 删除阶段

5.5.1 个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

5.5.2 收集阶段告知的个人信息使用目的达到后，立即删除个人信息；如需继续处理，要消除其中能够识别具体个人的内容；如需继续处理个人敏感信息，要获得个人信息主体的明示同意。

5.5.3 超出收集阶段告知的个人信息留存期限，要立即删除相关信息；对留存期限有

明确规定的，按相关规定执行。

5.5.4 个人信息管理者破产或解散时，若无法继续完成承诺的个人信息处理目的，要删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施。

网络产品和服务安全审查办法（试行）

（2017 年 5 月　国家网信办发布）

第一条　为提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条　关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。

第三条　坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其供应链进行网络安全审查。

第四条　网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括：

（一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；

（二）产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

（三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

（四）产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；

（五）其他可能危害国家安全的风险。

第五条　国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。

网络安全审查办公室具体组织实施网络安全审查。

第六条　网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。

第七条　国家依法认定网络安全审查第三方机构，承担网络安全审查中的第三方评价工作。

第八条　网络安全审查办公室按照国家有关要求、根据全国性行业协会建议和用户反映等，按程序确定审查对象，组织第三方机构、专家委员会对网络产品和服务进行网络安

全审查，并发布或在一定范围内通报审查结果。

第九条　金融、电信、能源、交通等重点行业和领域主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。

第十条　公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过网络安全审查。产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

第十一条　承担网络安全审查的第三方机构，应当坚持客观、公正、公平的原则，按照国家有关规定，参照有关标准，重点从产品和服务及其供应链的安全性、可控性，安全机制和技术的透明性等方面进行评价，并对评价结果负责。

第十二条　网络产品和服务提供者应当对网络安全审查工作予以配合，并对提供材料的真实性负责。

第三方机构等相关单位和人员对审查工作中获悉的信息等承担安全保密义务，不得用于网络安全审查以外的目的。

第十三条　网络安全审查办公室不定期发布网络产品和服务安全评估报告。

第十四条　网络产品和服务提供者认为第三方机构等相关单位和人员有失客观公正，或未能对审查工作中获悉的信息承担安全保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十五条　违反本办法规定的，依照有关法律法规予以处理。

第十六条　本办法自 2017 年 6 月 1 日起实施。

国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

（国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会公告 2017 年第 1 号）

为加强网络关键设备和网络安全专用产品安全管理，依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，现予以公布，自印发之日起施行。

一、列入《网络关键设备和网络安全专用产品目录》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。

二、网络关键设备和网络安全专用产品认证或者检测委托人，选择具备资格的机构进行安全认证或者安全检测。

三、网络关键设备、网络安全专用产品选择安全检测方式的，经安全检测符合要求后，由检测机构将网络关键设备、网络安全专用产品检测结果（含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品）依照相关规定分别报工业和信息化部、公安部。

选择安全认证方式的，经安全认证合格后，由认证机构将认证结果（含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品）依照相关规定报国家认证认可监督管理委员会。

国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一发布。

特此公告。

附件：网络关键设备和网络安全专用产品目录（第一批）

国家互联网信息办公室

工业和信息化部

公安部

国家认证认可监督管理委员会

2017 年 6 月 1 日

附件：网络关键设备和网络安全专用产品目录（第一批）

	设备或产品类别	范围
网络关键设备	1.路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55 万条
	2.交换机	整系统吞吐量(双向)≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器（机架式）	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时
	6. 防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥6Gbps

		最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统（IDS）	满检速率≥15Gbps 最大并发连接数≥500 万
	9.入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500 万
	10.安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
	11.反垃圾邮件产品	连接处理速率(连接/秒)＞100 平均延迟时间＜100ms
	12.网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC-E tpsE（每秒可交易数量）≥4500 个
	15. 网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10 级

国家认证认可监督管理委员会公告

（2018 年第 24 号）

关于网络关键设备和网络安全专用产品安全认证实施要求的公告

根据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》《关于发布＜网络关键设备和网络安全专用产品目录（第一批）＞的公告》（国家互联网信息办公室、工业和信息化部、公安部、国家认监委公告 2017 年第 1 号，以下简称 2017 年第 1 号公告），现将网络关键设备和网络安全专用产品安全认证实施要求予以公告。

一、目录内产品生产企业选择安全认证方式的，应向经确认的认证机构提出安全认证申请，认证机构依据《网络关键设备和网络安全专用产品安全认证实施规则》（由国家认监委另行发布）实施认证。为认证机构提供检测服务的实验室具体信息详见附件。

二、目录内产品如已获得经确认的认证机构颁发的产品认证证书且在有效期内的，相关生产企业可直接向该机构申请换发安全认证证书。

三、认证机构将认证结果（含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品）依照相关规定报国家认证认可监督管理委员会。发布方式按照 2017 年第 1 号公告执行。

附件：实验室名录

认监委

国家互联网信息办公室

2018 年 5 月 30 日

附件：实验室名录

序号	机构名称	对应法人单位	机构地址	联系方式
1	信息产业信息安全测评中心	中国电子科技集团公司第十五研究所	北京市海淀区北四环中路 211 号 邮编：100083	联系人：霍珊珊 电话：010-89056107 传真：010-89055529 E-mail：

				service@itstec.org.cn 网址：http: //www.itstec.org.cn
2	国家保密科技测评中心	国家保密科技测评中心	北京市海淀区交大东路甲 56 号 邮编：100044	联系人：曲天光 电话：010-55622970、 010-55622680 传真：010-55623954 E-mail：nsstec@126.com 网址：http: //www.isstec.org.cn
3	公安部计算机信息系统安全产品质量监督检验中心	公安部第三研究所	上海市岳阳路 76 号 邮编：200031	联系人：顾健 电话：021-64335070 传真：021-64335838 E-mail：mail@mctc.org.cn 网址：http: //www.mctc.org.cn
4	国家密码管理局商用密码检测中心	国家密码管理局商用密码检测中心	北京市丰台区靛厂路 7 号 邮编：100036	联系人：刘芳、侯北萍 电话：010-59703705、 010-59703719 传真：010-59703693 E-mail： mail@scctc.org.cn 网址：http: //www.scctc.org.cn
5	中国信息安全测评中心信息安全实验室	中国信息安全测评中心	北京市海淀区上地西路 8 号院 1 号楼 邮编：100085	联系人：张骁 电话：010-82341170 传真：010-82341100 E-mail： zhangx@itsec.gov.cn 网址：http: //www.itsec.gov.cn
6	北京信息安全测评中心	北京信息安全测评中心	北京市朝阳区北辰西路 12 号数字北京大厦 A 座 10 层北侧 邮编：100101	联系人：贺海 电话：010-84437931 传真：010-84437900 E-mail： hehai@bjeit.gov.cn

				网址：http://www.bjtec.org.cn
7	上海市信息安全测评认证中心	上海市信息安全测评认证中心	上海市陆家浜路1308号 邮编：200011	联系人：陈颖杰 电话：021-63789038 传真：021-63789039 E-mail：chenyj@shtec.org.cn 网址：http://www.shtec.org.cn
8	国家信息技术安全研究中心信息安全特种技术检测实验室	国家信息技术安全研究中心	北京市海淀区农大南路1号硅谷亮城2C座 邮编：100084	联系人：贾嘉 电话：010-59613742 传真：010-59613975 E-mail：jiajia@nitsrc.cn 网址：http://www.nitsc.cn

编号：CNCA-CCIS-2018

网络关键设备和网络安全专用产品安全认证实施规则

国家认证认可监督管理委员会发布

目 录

1.适用范围

本规则依据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》制定，规定了开展网络关键设备和网络安全专用产品安全认证的基本原则和要求。

本规则适用的网络关键设备和网络安全专用产品，应符合《国家互联网信息办公室、工业和信息化部、公安部、国家认监委关于发布<网络关键设备和网络安全专用产品目录（第一批）>的公告》（联合公告2017年第1号）中相应的范围要求描述（详见附件1）。

安全认证用标准依据有关主管部门的要求执行。

2.认证模式

型式试验 + 工厂检查 + 获证后监督

3.认证的基本环节

3.1 认证申请及受理

3.2 文档审核

3.3 型式试验委托及实施

3.4 工厂检查

3.5 认证结果评价与批准

3.6 获证后监督

4.认证实施

4.1 认证流程

认证委托人向认证机构申请认证，认证机构在接收到认证委托人的认证申请后，审查申请资料，确认合格后向认证委托人选择的实验室安排检测任务，并通知认证委托人根据要求抽样检测。实验室依据相关标准和/或技术规范进行检测，并在完成检测后向认证机构提交检测报告。认证机构对检测报告审查合格后，需要时由认证机构组织进行工厂检查。认证机构对型式试验、工厂检查结果进行认证决定，并在认证决定评价合格后向认证委托人颁发认证证书。认证机构组织对获证后的产品进行定期的监督。

4.2 认证申请及受理

认证委托人向认证机构递交认证申请，并按要求提交相关资料，认证机构对资料进行初审，确定认证委托人提交资料满足要求后，受理该申请。

4.2.1 认证的单元划分

按产品型号/版本申请认证，若产品的关键件相同的可作为一个单元申请认证，由认证机构根据认证要求对产品关键件做出规定。

以多于一个型号/版本的产品为同一认证单元申请认证时，认证委托人应提交同一认证单元中型号/版本间的差异说明及相关测试报告。

4.2.2 申请资料要求

认证委托人在申请安全认证时，应至少提交以下资料：

1） 申请基本信息：

- 认证申请书；
- 认证委托人声明；
- 相关法律地位证明材料（复印件）；
- 质量体系方面有关的文件。

2） 有关技术指标参数声明及支撑材料（依据附件 1“范围”中的内容）。

3） 产品相关说明：

- 中文产品功能说明书和/或使用手册；
- 认证标准的适用性说明；
- 产品研制主要技术人员情况表；
- 产品测试技术人员情况表；
- 产品测试使用的主要设备表；
- 中文铭牌和警告标记；
- 同一认证单元中型号/版本间的差异说明及相关测试报告（如适用）；
- 产品密码检测合格证书（如适用）。

4） 安全保障要求方面的文档：

- 配置管理；
- 交付与运行；
- 开发；
- 指导性文档；
- 测试。

5） 安全功能相关说明文件。

6） 认证机构要求的其他资料。

4.3 文档审核

对认证委托人提交的资料和文档，根据相关标准和/或该产品的技术规范进行审核。

4.4 型式试验委托及实施

4.4.1 型式试验抽样

4.4.1.1 抽样要求

由认证机构安排对申请认证的产品按型号/版本进行抽样,样品应在生产企业生产的产品中（包括生产线、仓库、市场）随机抽取。一般每种产品抽样 2 套，如有特殊需求可增加样品数量。

认证委托人将样品递送至实验室，并对样品负责。

认证委托人应根据型式试验的要求，提供相应的说明及辅助设备。

4.4.1.2 样品及相关资料的处置

认证结束后，认证委托人可向实验室申请取回型式试验样品，相关申请资料由认证机构、实验室妥善处置。

4.4.2 型式试验依据

按相应产品有关国家标准的要求执行。

4.4.3 型式试验报告的提交

型式试验完成后，实验室根据认证机构的要求出具型式试验报告并提交给认证机构。

4.5 工厂检查

4.5.1 审核内容

工厂检查的内容为信息安全保障能力、质量保证能力、产品一致性检查。

4.5.1.1 信息安全保障能力

由认证机构派检查员对制造商、生产企业按照附件 2（信息安全保障能力基本要求）实施审核（当认证依据的国家标准涵盖安全保障能力要求时，则按相应国家标准实施）。

4.5.1.2 质量保证能力

由认证机构派检查员对生产企业按照附件 3（质量保证能力基本要求）及认证机构制定的补充检查要求进行检查。

4.5.1.3 产品一致性

工厂检查时，应在生产现场对申请认证的产品进行一致性检查。重点检查以下内容：

1）认证产品的铭牌、包装上所标明的及运行时所显示的产品名称、型号/版本号与型式试验报告上所标明的内容是否一致；

2）认证产品所用的软件、硬件应与型式试验合格的样品一致；

3）非认证的产品是否违规标贴了认证标识。

4.5.2 工厂检查时间

由认证机构根据认证实施需要安排工厂检查。人日数根据所申请认证产品的单元数量确定，并适当考虑制造商、生产企业的规模及产品的安全级别，一般每个场所为 2 至 6 个人日。

4.6 认证结果评价与批准

认证机构负责对型式试验、工厂检查结果等进行综合评价，做出认证决定，通过认证决定的，由认证机构对认证委托人颁发认证证书（每一个认证单元颁发一张认证证书）。如认证决定过程中发现不符合认证要求项，允许限期（不超过 3 个月）整改，如期完成整改后，认证机构采取适当方式对整改结果进行确认，重新执行认证决定过程。

4.7 获证后监督

4.7.1 监督的频次

监督频次一般为一年一次，当有特别规定时，认证机构可调整监督频次。必要时，认证机构可采取事先不通知的方式进行监督。

如果发生下述情况之一可增加监督频次：

1）获证产品出现严重质量问题时,或者用户提出投诉并经查实为证书持有者责任时；

2）认证机构有足够理由对获证产品与规定的标准要求的符合性提出质疑时；

3）有足够信息表明制造商、生产企业因组织机构、生产条件、质量管理体系等发生变更，从而可能影响产品质量时。

4.7.2 监督的内容

获证后监督采用工厂检查的方式进行，主要针对信息安全保障能力、认证产品一致性和质量保证能力进行检查。必要时可以抽取样品送实验室检测，需要进行抽样检测时，按 4.4.1.1 要求实施抽样。初次认证申请时的检测项目都可以作为监督时的检测项目，认证机构可根据具体情况进行部分或全部项目的检测。样品的检测一般由认证机构指定的检测

实验室在20个工作日内完成。

4.7.3 获证后监督结果的评价

监督复查合格后，可以继续保持认证证书、使用认证标志。对监督复查时发现的不符合项应在3个月内完成纠正措施。逾期将撤销认证证书、停止使用认证标志，并对外公告。

5.认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的工作日，一般在90个工作日内。整改时间不计算在内。

6.认证证书

6.1 证书的有效性

证书有效期5年。在有效期内，通过每年对获证后的产品进行监督确保认证证书的有效性。

6.2 认证证书的变更

6.2.1 变更的申请

获证后的产品，如果其制造商、生产企业、证书持有者等发生变化时，应向认证机构提出变更申请。

6.2.2 变更申请的评价与批准

认证机构根据变更的内容和提供的资料进行文件审核,需要时安排型式试验和/或工厂检查，认证评价通过后予以变更证书。

6.2.3 证书的有效期

证书在进行变更后，其有效期与原证书一致。

6.3 认证证书覆盖产品的扩展

6.3.1 认证证书覆盖产品扩展申请

认证证书持有者需要增加已经获得认证产品的认证范围时，应向认证机构提出扩展申请，并提交扩展产品和原认证产品之间的差异说明。

6.3.2 认证证书覆盖产品扩展的评价与批准

认证机构应核查扩展产品与原认证产品的一致性，确认原认证结果对扩展产品的有效性,需要时应针对差异做补充型式试验和/或工厂检查,并根据认证证书持有者的要求单独颁发认证证书或换发认证证书。

6.3.3 证书的有效期

证书在进行扩展后，其有效期与原证书一致。

6.4 认证证书的暂停、注销和撤销

参照《强制性产品认证证书注销、暂停、撤销实施规则》的要求执行。在认证证书暂停期间及认证证书注销和撤销后，获证机构不得继续使用证书。

7.认证标志的使用

7.1 认证标志的样式

7.2 认证标志的使用

认证标志在使用时可以等比例的放大或缩小。但是，不允许变形或变色。

7.3 加施方式

可以采用统一印制的标准规格标志、模压、铭牌印刷、软件加施等方式。

7.4 标志位置

应在产品本体的铭牌附近加施认证标志。

软件产品应在其软件包装/载体上加施认证标志，如该软件产品不使用包装/载体，则应在软件使用的《许可协议》中的显著位置明确该产品已获认证机构认证。

附件 1

网络关键设备和网络安全专用产品目录

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量（双向）≥12Tbps 整系统路由表容量≥55万条
	2. 交换机	整系统吞吐量（双向）≥30Tbps

		整系统包转发率≥10Gpps
	3. 服务器（机架式）	CPU数量≥8个 单CPU内核数≥14个 内存容量≥256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤0.08微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1小时
	6. 防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300万 每秒新建连接数≥25万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥6Gbps 最大HTTP并发连接数≥200万
	8. 入侵检测系统（IDS）	满检速率≥15Gbps 最大并发连接数≥500万
	9. 入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500万
	10. 安全隔离与信息交换产品（网闸）	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率（连接/秒）>100 平均延迟时间<100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描IP数量≥60个
	14. 安全数据库系统	TPC-E tpsE(每秒可交易数量)≥4500个
	15 网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10级

附件 2

信息安全保障能力基本要求

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.2 安全执行功能规范
	ADV_TDS.1 基础设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.2 CM系统的使用
	ALC_CMS.2 部分TOE CM覆盖
	ALC_DEL.1 交付程序

附件 3

质量保证能力基本要求

为保证批量生产的认证产品与型式试验样品的一致性，生产企业应满足本文件规定的质量保证能力基本要求。

1.职责和资源

1.1 职责

生产企业应规定与质量活动有关的各类人员职责及相互关系，且生产企业应在组织内指定一名质量负责人，无论该成员在其他方面的职责如何，应具有以下方面的职责和权限：

a）负责建立满足本文件要求的质量体系，并确保其实施和保持；

b）确保加贴认证标志的产品符合认证标准的要求；

c）建立文件化的程序，确保认证标志的妥善保管和使用；

d）建立文件化的程序，确保不合格品和获证产品变更后未经认证机构确认，不加贴认证标志。

质量负责人应具有充分的能力胜任本职工作。

1.2 资源

生产企业应配备必须的生产设备和检测设备以满足稳定生产符合本规则中规定的标准要求的产品；应配备相应的人力资源，确保从事对产品质量有影响工作的人员具备必要的能力；建立并保持适宜产品生产、试验、储存等必备的环境。

2.认证产品一致性

a）生产企业应对现场的产品与型式试验样品的一致性进行控制，以使认证产品持续符合规定的要求；

b）生产企业应建立产品变更控制程序，认证产品的变更在实施前应向认证机构申报并获得批准后方可执行。

3.认证产品外购部件或外包软件模块管理

3.1 外购部件供应商或软件模块的外包商的控制

a)生产企业应制定外购部件供应商或软件模块外包商的选择、评定和日常管理的程序，以确保供应商提供的部件或软件外包商提供的软件模块满足要求；

b）生产企业应保存对供应商或软件外包商的选择评价和日常管理记录。

3.2 外购部件或外包软件模块的验证

a)生产企业应建立并保持对供应商提供的部件或软件外包商提供的软件模块的验证程序及定期确认程序，以确保部件或软件模块满足认证所规定的要求；

b）生产企业应保存部件或外包软件模块，或者它们的验证记录、确认记录及供应商或软件外包商提供的合格证明及有关数据等。

国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部关于发布《云计算服务安全评估办法》的公告

（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部公告2019年第2号）

为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部制定了《云计算服务安全评估办法》，现予以发布。

附件：云计算服务安全评估办法

国家互联网信息办公室

国家发展和改革委员会

工业和信息化部

财政部

2019年7月2日

云计算服务安全评估办法

第一条　为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，制定本办法。

第二条　云计算服务安全评估坚持事前评估与持续监督相结合，保障安全与促进应用相统一，依据有关法律法规和政策规定，参照国家有关网络安全标准，发挥专业技术机构、专家作用，客观评价、严格监督云计算服务平台（以下简称“云平台”）的安全性、可控性，为党政机关、关键信息基础设施运营者采购云计算服务提供参考。

本办法中的云平台包括云计算服务软硬件设施及其相关管理制度等。

第三条　云计算服务安全评估重点评估以下内容：

（一）云平台管理运营者（以下简称“云服务商”）的征信、经营状况等基本情况；

（二）云服务商人员背景及稳定性，特别是能够访问客户数据、能够收集相关元数据的人员；

（三）云平台技术、产品和服务供应链安全情况；

（四）云服务商安全管理能力及云平台安全防护情况；

（五）客户迁移数据的可行性和便捷性；

（六）云服务商的业务连续性；

（七）其他可能影响云服务安全的因素。

第四条　国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、财政部建立云计算服务安全评估工作协调机制（以下简称“协调机制”），审议云计算服务安全评估政策文件，批准云计算服务安全评估结果，协调处理云计算服务安全评估有关重要事项。

云计算服务安全评估工作协调机制办公室（以下简称“办公室”）设在国家互联网信息办公室网络安全协调局。

第五条　云服务商可申请对面向党政机关、关键信息基础设施提供云计算服务的云平台进行安全评估。

第六条　申请安全评估的云服务商应向办公室提交以下材料：

（一）申报书；

（二）云计算服务系统安全计划；

（三）业务连续性和供应链安全报告；

（四）客户数据可迁移性分析报告；

（五）安全评估工作需要的其他材料。

第七条　办公室受理云服务商申请后，组织专业技术机构参照国家有关标准对云平台进行安全评价。

第八条　专业技术机构应坚持客观、公正、公平的原则，按照国家有关规定，在办公室指导监督下，参照《云计算服务安全指南》《云计算服务安全能力要求》等国家标准，重点评价本办法第三条所述内容，形成评价报告，并对评价结果负责。

第九条　办公室在专业技术机构安全评价基础上，组织云计算服务安全评估专家组进行综合评价。

第十条　云计算服务安全评估专家组根据云服务商申报材料、评价报告等，综合评价云计算服务的安全性、可控性，提出是否通过安全评估的建议。

第十一条　云计算服务安全评估专家组的建议经协调机制审议通过后，办公室按程序

报国家互联网信息办公室核准。

云计算服务安全评估结果由办公室发布。

第十二条　云计算服务安全评估结果有效期3年。有效期届满需要延续保持评估结果的，云服务商应在届满前至少6个月向办公室申请复评。

有效期内，云服务商因股权变更、企业重组等导致实控人或控股权发生变化的，应重新申请安全评估。

第十三条　办公室通过组织抽查、接受举报等形式，对通过评估的云平台开展持续监督，重点监督有关安全控制措施有效性、重大变更、应急响应、风险处置等内容。

通过评估的云平台已不再满足要求的，经协调机制审议、国家互联网信息办公室核准后撤销通过评估的结论。

第十四条　通过评估的云平台停止提供服务时，云服务商应至少提前6个月通知客户和办公室，并配合客户做好迁移工作。

第十五条　云服务商对所提供申报材料的真实性负责。在评估过程中拒绝按要求提供材料或故意提供虚假材料的，按评估不通过处理。

第十六条　未经云服务商同意，参与评估工作的相关机构和人员不得披露云服务商提交的未公开材料以及评估工作中获悉的其他非公开信息，不得将云服务商提供的信息用于评估以外的目的。

第十七条　本办法自2019年9月1日起施行。

《云计算服务安全评估办法》有关问题解答

（2019 年 7 月 22 日）

1、组织开展云计算服务安全评估的目的是什么？

答：开展云计算服务安全评估，是为了提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，降低采购使用云计算服务带来的网络安全风险，增强党政机关、关键信息基础设施运营者将业务及数据向云服务平台迁移的信心。

2、云计算服务安全评估的对象是什么？

答：云计算服务安全评估是依据云服务商申请，对面向党政机关、关键信息基础设施提供云计算服务的云平台进行的安全评估。同一云服务商运营的不同云平台，需要分别申请安全评估。

3、何时起云服务商可申请评估？需要提交哪些材料？

答：自 2019 年 9 月 1 日起云服务商可以正式提交云计算服务安全评估申请。需要提交的材料包括申报书、云计算服务系统安全计划、业务连续性和供应链安全报告、客户数据可迁移性分析报告等。有关申报材料模版将在中国网信网提供下载。

4、已通过党政部门云计算服务网络安全审查的云平台，是否还需要申请云计算服务安全评估？

答：前期已经通过党政部门云计算服务网络安全审查的云平台，视同为已通过云计算服务安全评估，不需要再重新申请。

5、云计算服务安全评估主要参照哪些标准？

答：云计算服务安全评估主要参照国家标准《云计算服务安全能力要求》、《云计算服务安全指南》，其中《云计算服务安全能力要求》从系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境安全等方面提出要求。

6、云计算服务安全评估有哪些主要环节？

答：主要包括申报、受理、专业技术机构评价、云计算服务安全评估专家组综合评价、云计算服务安全评估工作协调机制审议、国家互联网信息办公室核准、评估结果发布、持续监督等环节。

7、云计算服务安全评估结果在哪里查询？有效期多长时间？

答：评估结果将由国家互联网信息办公室网络安全协调局在中国网信网公布。评估结果有效期为3年。

8、云计算服务安全评估如何保护被评估方的商业秘密和知识产权？

答：云计算服务安全评估过程中，参与评估工作的单位和人员对云服务商提交的非公开材料或在评估中获悉的非公开信息承担保密义务，严格保护云服务商的商业秘密和知识产权。如果云服务商认为有关单位和人员未能承担保密义务的，可以向国家互联网信息办公室或有关部门举报。

9、关于云计算服务安全评估问题可向谁咨询？

答：有关云计算服务安全评估的其他具体事项，可发送电子邮件到yunpinggu@cac.gov.cn或拨打010-55635861咨询。

来源：工业和信息化部

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。

工信部印发《工业控制系统信息安全事件应急管理工作指南》

为贯彻落实《中华人民共和国网络安全法》《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号），指导做好工业控制系统信息安全事件应急管理相关工作，保障工业控制系统信息安全，2017年5月31日，工业和信息化部印发《工业控制系统信息安全事件应急管理工作指南》。《指南》全文如下：

工业控制系统信息安全事件应急管理工作指南

第一章 总 则

第一条 为加强工业控制系统信息安全（以下简称工控安全）应急工作管理，建立健全工控安全应急工作机制，提高应对工控安全事件的组织协调和应急处置能力，预防和减少工控安全事件造成的损失和危害，保障工业生产正常运行，维护国家经济安全和人民生命财产安全,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》以及《国务院关于深化制造业与互联网融合发展的指导意见》等法规政策，制定本指南。

第二条 本指南适用于工业和信息化主管部门、工业企业开展工控安全应急管理工作。

第三条 工控安全事件是指由于人为、软硬件缺陷或故障、自然灾害等原因，对工业控制系统、工业控制系统数据造成或者可能造成严重危害，影响正常工业生产的事件。

第四条 坚持政府指导、企业主体，坚持预防为主、平战结合，坚持快速反应、科学处置，充分发挥各方力量，共同做好工控安全事件的预防和处置工作。

第二章 组织机构与职责

第五条 工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业做好工控安全应急管理工作。

第六条 地方工业和信息化主管部门负责指导本地区工控安全应急管理工作。

第七条 工控安全应急技术机构负责具体开展工控安全风险监测、态势研判、威胁预警、事件处置等工作。

第八条 工业企业负有工控安全主体责任，应建立健全工控安全责任制，负责本单位工

控安全应急管理工作，落实人财物保障。

第三章　工作机制

第九条 工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业等建立工控安全联络员机制，指定工控安全应急工作联络员，报工业和信息化部备案，联络员和联络方式发生变化时需及时报工业和信息化部。工业和信息化部根据工作需要组织召开联络员会议。

第十条 地方工业和信息化主管部门指导本地区应急技术机构、工业企业建立工控安全应急值守机制，实行领导带班、专人值守工作制度，做好工控安全风险、威胁、事件信息日常监测和报告工作。应急响应状态下，实行“7×24”小时值守，加强信息监测、收集与研判，做好信息跟踪报告。

第四章　监测通报

第十一条 工业和信息化部指导国家工业信息安全发展研究中心等技术机构，组织开展全国工控安全风险监测、预警通报等工作，提升情报搜集、态势分析、风险评估和信息共享能力。

地方工业和信息化主管部门组织开展本地区工控安全风险监测工作。工业企业组织开展本单位工控安全风险监测工作。

第十二条 地方工业和信息化主管部门、工业企业定期将重要监测信息报国家工业信息安全发展研究中心，国家工业信息安全发展研究中心负责汇总、整理和研判，并将结果报工业和信息化部；针对可能超出本地区应对能力范围的安全风险和事件信息，及时上报，必要时工业和信息化部协调应急技术机构提供支持。

第十三条 工业和信息化部对可能影响我国工业控制系统的重大漏洞和风险，及时向有关行业、地区和工业企业发布情况通报。

第五章　敏感时期应急管理

第十四条 在国家重要活动、会议等敏感时期，工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业开展工控安全事件预防和应急管理工作。

第十五条 地方工业和信息化主管部门、工业企业加强工控安全监测和风险研判，对可能造成重大影响的风险和事件信息应及时上报，必要时实行 24 小时零报告制度。重点单位、重要部位实施 24 小时值守，保持通信联络畅通。相关工业企业应加强对工业控制系统的巡

检巡查，原则上不在敏感时期对工业控制系统进行调整或升级。

第六章　应急处置

第十六条 对于可能发生或已经发生的工控安全事件，工业企业应立即开展应急处置，采取科学有效方法及时施救，力争将损失降到最小，尽快恢复受损工业控制系统的正常运行。当事发工业企业应急处置力量不足时，可请求上级主管部门协调应急技术机构提供支援。

第十七条 有关地方工业和信息化主管部门和工业企业应及时向工业和信息化部报告事态发展变化情况和事件处置进展情况。报告信息一般包括以下要素：事件涉及的工业控制系统名称及运营管理单位、时间、地点、原因、来源、类型、性质、危害、影响范围、发展趋势、处置措施等。

第十八条 工业和信息化部指导、督促事发企业开展应急处置工作，必要时派出工作组赴现场指挥协调应急处置工作，协调应急技术机构提供技术支援。

第十九条 应急处置结束、系统恢复运行后，相关工业企业要尽快消除事件造成的不良影响，做好事件分析总结工作，总结报告应在 30 天内以书面形式报工业和信息化部。

第二十条 对于工控安全事件性质、起因、范围、损失等，工业和信息化主管部门和相关人员应做好舆论宣传和引导工作。

第七章　保障措施

第二十一条 工业和信息化部、地方工业和信息化主管部门、工业企业制定本级工控安全事件应急预案，定期组织应急演练。

第二十二条 工业和信息化部建立国家工控安全应急专家组，为工控安全应急管理提供技术咨询和决策支持。地方工业和信息化主管部门建立本地区工控安全应急专家组，充分发挥专家在应急管理工作中的作用。

第二十三条 加强对工控安全事件应急装备和工具的储备，及时调整、升级软硬件工具，建设完善工控安全事件应急技术服务平台，不断增强应急技术支撑能力。

第二十四条 各有关部门应积极利用现有政策和资金渠道，申请新增预算，支持工控安全应急技术机构建设、专家队伍建设、基础平台建设、技术研发、应急演练、物资保障等，为工控安全应急管理工作提供必要的经费支持。

第二十五条 本指南自 2017 年 7 月 1 日起施行。

网络安全漏洞管理规定（征求意见稿）

第一条 为规范网络安全漏洞（以下简称漏洞）报告和信息发布等行为，保证网络产品、服务、系统的漏洞得到及时修补，提高网络安全防护水平，根据《国家安全法》《网络安全法》，制定本规定。

第二条 中华人民共和国境内网络产品、服务提供者和网络运营者，以及开展漏洞检测、评估、收集、发布及相关竞赛等活动的组织（以下简称第三方组织）或个人，应当遵守本规定。

第三条 网络产品、服务提供者和网络运营者发现或获知其网络产品、服务、系统存在漏洞后，应当遵守以下规定：

（一）立即对漏洞进行验证，对相关网络产品应当在90日内采取漏洞修补或防范措施，对相关网络服务或系统应当在10日内采取漏洞修补或防范措施；

（二）需要用户或相关技术合作方采取漏洞修补或防范措施的，应当在对相关网络产品、服务、系统采取漏洞修补或防范措施后5日内，将漏洞风险及用户或相关技术合作方需采取的修补或防范措施向社会发布或通过客服等方式告知所有可能受影响的用户和相关技术合作方，提供必要的技术支持，并向工业和信息化部网络安全威胁信息共享平台报送相关漏洞情况。

第四条 工业和信息化部、公安部和有关行业主管部门按照各自职责组织督促网络产品、服务提供者和网络运营者采取漏洞修补或防范措施。

第五条 工业和信息化部、公安部、国家互联网信息办公室等有关部门实现漏洞信息实时共享。

第六条 第三方组织或个人通过网站、媒体、会议等方式向社会发布漏洞信息，应当遵循必要、真实、客观、有利于防范和应对网络安全风险的原则，并遵守以下规定：

（一）不得在网络产品、服务提供者和网络运营者向社会或用户发布漏洞修补或防范措施之前发布相关漏洞信息；

（二）不得刻意夸大漏洞的危害和风险；

（三）不得发布和提供专门用于利用网络产品、服务、系统漏洞从事危害网络安全活动的方法、程序和工具；

（四）应当同步发布漏洞修补或防范措施。

第七条 第三方组织应当加强内部管理，履行下列管理义务，防范漏洞信息泄露和内部人员违规发布漏洞信息：

（一）明确漏洞管理部门和责任人；

（二）建立漏洞信息发布内部审核机制；

（三）采取防范漏洞信息泄露的必要措施；

（四）定期对内部人员进行保密教育；

（五）制定内部问责制度。

第八条 网络产品、服务提供者和网络运营者未按本规定采取漏洞修补或防范措施并向社会或用户发布的，由工业和信息化部、公安部等有关部门按职责依据《网络安全法》第五十六条、第五十九条、第六十条等规定组织对其进行约谈或给予行政处罚。

第九条 第三方组织违反本规定向社会发布漏洞信息，由工业和信息化部、公安部等有关部门组织对其进行约谈，或依据《网络安全法》第六十二条、第六十三条等规定给予行政处罚；构成犯罪的，依法追究刑事责任；给网络产品、服务提供者和网络运营者造成经济或名誉损害的，依法承担民事责任。

第十条 鼓励第三方组织和个人获知网络产品、服务、系统存在的漏洞后，及时向国家信息安全漏洞共享平台、国家信息安全漏洞库等漏洞收集平台报送有关情况。漏洞收集平台应当遵守本规定第六条、第七条规定。

第十一条　任何组织或个人发现涉嫌违反本规定的情形，有权向工业和信息化部、公安部举报。

第十二条　本规定自印发之日起施行。

最高人民法院、最高人民检察院公告

《最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释》已于2013年9月5日由最高人民法院审判委员会第1589次会议、2013年9月2日由最高人民检察院第十二届检察委员会第9次会议通过，现予公布，自2013年9月10日起施行。

最高人民法院

最高人民检察院

2013年9月6日

最高人民法院、最高人民检察院关于办理利用信息网络实施诽谤等刑事案件适用法律若干问题的解释

（法释〔2013〕21号 2013年9月5日最高人民法院审判委员会第1589次会议、2013年9月2日

最高人民检察院第十二届检察委员会第9次会议通过）

为保护公民、法人和其他组织的合法权益，维护社会秩序，根据《中华人民共和国刑法》《全国人民代表大会常务委员会关于维护互联网安全的决定》等规定，对办理利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等刑事案件适用法律的若干问题解释如下：

第一条　具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“捏造事实诽谤他人”：

（一）捏造损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

（二）将信息网络上涉及他人的原始信息内容篡改为损害他人名誉的事实，在信息网络上散布，或者组织、指使人员在信息网络上散布的；

明知是捏造的损害他人名誉的事实，在信息网络上散布，情节恶劣的，以“捏造事实诽谤他人”论。

第二条　利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第一款规定的“情节严重”：

（一）同一诽谤信息实际被点击、浏览次数达到五千次以上，或者被转发次数达到五百次以上的；

（二）造成被害人或者其近亲属精神失常、自残、自杀等严重后果的；

（三）二年内曾因诽谤受过行政处罚，又诽谤他人的；

（四）其他情节严重的情形。

第三条　利用信息网络诽谤他人，具有下列情形之一的，应当认定为刑法第二百四十六条第二款规定的“严重危害社会秩序和国家利益”：

（一）引发群体性事件的；

（二）引发公共秩序混乱的；

（三）引发民族、宗教冲突的；

（四）诽谤多人，造成恶劣社会影响的；

（五）损害国家形象，严重危害国家利益的；

（六）造成恶劣国际影响的；

（七）其他严重危害社会秩序和国家利益的情形。

第四条　一年内多次实施利用信息网络诽谤他人行为未经处理，诽谤信息实际被点击、浏览、转发次数累计计算构成犯罪的，应当依法定罪处罚。

第五条　利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第（二）项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第（四）项的规定，以寻衅滋事罪定罪处罚。

第六条　以在信息网络上发布、删除等方式处理网络信息为由，威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

第七条　违反国家规定，以营利为目的，通过信息网络有偿提供删除信息服务，或者明知是虚假信息，通过信息网络有偿提供发布信息等服务，扰乱市场秩序，具有下列情形之

一的，属于非法经营行为“情节严重”，依照刑法第二百二十五条第（四）项的规定，以非法经营罪定罪处罚：

（一）个人非法经营数额在五万元以上，或者违法所得数额在二万元以上的；

（二）单位非法经营数额在十五万元以上，或者违法所得数额在五万元以上的。

实施前款规定的行为，数额达到前款规定的数额五倍以上的，应当认定为刑法第二百二十五条规定的“情节特别严重”。

第八条　明知他人利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营等犯罪，为其提供资金、场所、技术支持等帮助的，以共同犯罪论处。

第九条　利用信息网络实施诽谤、寻衅滋事、敲诈勒索、非法经营犯罪，同时又构成刑法第二百二十一条规定的损害商业信誉、商品声誉罪，第二百七十八条规定的煽动暴力抗拒法律实施罪，第二百九十一条之一规定的编造、故意传播虚假恐怖信息罪等犯罪的，依照处罚较重的规定定罪处罚。

第十条　本解释所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

最高人民法院公告

《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》已于2012年11月26日由最高人民法院审判委员会第1561次会议通过，现予公布，自2013年1月1日起施行。

最高人民法院

2012年12月17日

最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定

（法释〔2012〕20号）

为正确审理侵害信息网络传播权民事纠纷案件，依法保护信息网络传播权，促进信息网络产业健康发展，维护公共利益，根据《中华人民共和国民法通则》、《中华人民共和国侵权责任法》、《中华人民共和国著作权法》、《中华人民共和国民事诉讼法》等有关法律规定，结合审判实际，制定本规定。

第一条　人民法院审理侵害信息网络传播权民事纠纷案件，在依法行使裁量权时，应当兼顾权利人、网络服务提供者和社会公众的利益。

第二条　本规定所称信息网络，包括以计算机、电视机、固定电话机、移动电话机等电子设备为终端的计算机互联网、广播电视网、固定通信网、移动通信网等信息网络，以及向公众开放的局域网络。

第三条　网络用户、网络服务提供者未经许可，通过信息网络提供权利人享有信息网络传播权的作品、表演、录音录像制品，除法律、行政法规另有规定外，人民法院应当认定其构成侵害信息网络传播权行为。

通过上传到网络服务器、设置共享文件或者利用文件分享软件等方式，将作品、表演、录音录像制品置于信息网络中，使公众能够在个人选定的时间和地点以下载、浏览或者其他方式获得的，人民法院应当认定其实施了前款规定的提供行为。

第四条　有证据证明网络服务提供者与他人以分工合作等方式共同提供作品、表演、

录音录像制品，构成共同侵权行为的，人民法院应当判令其承担连带责任。网络服务提供者能够证明其仅提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务，主张其不构成共同侵权行为的，人民法院应予支持。

第五条　网络服务提供者以提供网页快照、缩略图等方式实质替代其他网络服务提供者向公众提供相关作品的，人民法院应当认定其构成提供行为。

前款规定的提供行为不影响相关作品的正常使用，且未不合理损害权利人对该作品的合法权益，网络服务提供者主张其未侵害信息网络传播权的，人民法院应予支持。

第六条　原告有初步证据证明网络服务提供者提供了相关作品、表演、录音录像制品，但网络服务提供者能够证明其仅提供网络服务，且无过错的，人民法院不应认定为构成侵权。

第七条　网络服务提供者在提供网络服务时教唆或者帮助网络用户实施侵害信息网络传播权行为的，人民法院应当判令其承担侵权责任。

网络服务提供者以言语、推介技术支持、奖励积分等方式诱导、鼓励网络用户实施侵害信息网络传播权行为的，人民法院应当认定其构成教唆侵权行为。

网络服务提供者明知或者应知网络用户利用网络服务侵害信息网络传播权，未采取删除、屏蔽、断开链接等必要措施，或者提供技术支持等帮助行为的，人民法院应当认定其构成帮助侵权行为。

第八条　人民法院应当根据网络服务提供者的过错，确定其是否承担教唆、帮助侵权责任。网络服务提供者的过错包括对于网络用户侵害信息网络传播权行为的明知或者应知。

网络服务提供者未对网络用户侵害信息网络传播权的行为主动进行审查的，人民法院不应据此认定其具有过错。

网络服务提供者能够证明已采取合理、有效的技术措施，仍难以发现网络用户侵害信息网络传播权行为的，人民法院应当认定其不具有过错。

第九条　人民法院应当根据网络用户侵害信息网络传播权的具体事实是否明显，综合考虑以下因素，认定网络服务提供者是否构成应知：

（一）基于网络服务提供者提供服务的性质、方式及其引发侵权的可能性大小，应当具备的管理信息的能力；

（二）传播的作品、表演、录音录像制品的类型、知名度及侵权信息的明显程度；

（三）网络服务提供者是否主动对作品、表演、录音录像制品进行了选择、编辑、修改、推荐等；

（四）网络服务提供者是否积极采取了预防侵权的合理措施；

（五）网络服务提供者是否设置便捷程序接收侵权通知并及时对侵权通知作出合理的反应；

（六）网络服务提供者是否针对同一网络用户的重复侵权行为采取了相应的合理措施；

（七）其他相关因素。

第十条　网络服务提供者在提供网络服务时，对热播影视作品等以设置榜单、目录、索引、描述性段落、内容简介等方式进行推荐，且公众可以在其网页上直接以下载、浏览或者其他方式获得的，人民法院可以认定其应知网络用户侵害信息网络传播权。

第十一条　网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。

网络服务提供者针对特定作品、表演、录音录像制品投放广告获取收益，或者获取与其传播的作品、表演、录音录像制品存在其他特定联系的经济利益，应当认定为前款规定的直接获得经济利益。网络服务提供者因提供网络服务而收取一般性广告费、服务费等，不属于本款规定的情形。

第十二条　有下列情形之一的，人民法院可以根据案件具体情况，认定提供信息存储空间服务的网络服务提供者应知网络用户侵害信息网络传播权：

（一）将热播影视作品等置于首页或者其他主要页面等能够为网络服务提供者明显感知的位置的；

（二）对热播影视作品等的主题、内容主动进行选择、编辑、整理、推荐，或者为其设立专门的排行榜的；

（三）其他可以明显感知相关作品、表演、录音录像制品为未经许可提供，仍未采取合理措施的情形。

第十三条　网络服务提供者接到权利人以书信、传真、电子邮件等方式提交的通知，未及时采取删除、屏蔽、断开链接等必要措施的，人民法院应当认定其明知相关侵害信息网络传播权行为。

第十四条　人民法院认定网络服务提供者采取的删除、屏蔽、断开链接等必要措施是否及时，应当根据权利人提交通知的形式，通知的准确程度，采取措施的难易程度，网络服务的性质，所涉作品、表演、录音录像制品的类型、知名度、数量等因素综合判断。

第十五条　侵害信息网络传播权民事纠纷案件由侵权行为地或者被告住所地人民法院管辖。侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地。侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

第十六条　本规定施行之日起，《最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释》（法释〔2006〕11 号）同时废止。

本规定施行之后尚未终审的侵害信息网络传播权民事纠纷案件，适用本规定。本规定施行前已经终审，当事人申请再审或者按照审判监督程序决定再审的，不适用本规定。

最高人民法院、最高人民检察院、公安部、司法部关于印发《关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见》的通知

各省、自治区、直辖市高级人民法院、人民检察院、公安厅（局）、司法厅（局），解放军军事法院、军事检察院，新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局、司法局：

为认真贯彻落实中央开展扫黑除恶专项斗争的部署要求，正确理解和适用最高人民法院、最高人民检察院、公安部、司法部《关于办理黑恶势力犯罪案件若干问题的指导意见》，最高人民法院、最高人民检察院、公安部、司法部研究制定了《关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见》。现印发给你们，请认真贯彻执行。

最高人民法院

最高人民检察院

公安部

司法部

2019 年 7 月 23 日

最高人民法院 最高人民检察院 公安部 司法部关于办理利用信息网络实施黑恶势力犯罪刑事案件若干问题的意见

为认真贯彻中央关于开展扫黑除恶专项斗争的部署要求，正确理解和适用最高人民法院、最高人民检察院、公安部、司法部《关于办理黑恶势力犯罪案件若干问题的指导意见》（法发〔2018〕1 号，以下简称《指导意见》），根据刑法、刑事诉讼法、网络安全法及有关司法解释、规范性文件的规定，现对办理利用信息网络实施黑恶势力犯罪案件若干问题提出以下意见：

一、总体要求

1. 各级人民法院、人民检察院、公安机关及司法行政机关应当统一执法思想、提高执

法效能，坚持“打早打小”，坚决依法严厉惩处利用信息网络实施的黑恶势力犯罪，有效维护网络安全和经济、社会生活秩序。

2. 各级人民法院、人民检察院、公安机关及司法行政机关应当正确运用法律，严格依法办案，坚持“打准打实”，认真贯彻落实宽严相济刑事政策，切实做到宽严有据、罚当其罪，实现政治效果、法律效果和社会效果的统一。

3. 各级人民法院、人民检察院、公安机关及司法行政机关应当分工负责，互相配合、互相制约，切实加强与相关行政管理部门的协作，健全完善风险防控机制，积极营造线上线下社会综合治理新格局。

二、依法严惩利用信息网络实施的黑恶势力犯罪

4. 对通过发布、删除负面或虚假信息，发送侮辱性信息、图片，以及利用信息、电话骚扰等方式，威胁、要挟、恐吓、滋扰他人，实施黑恶势力违法犯罪的，应当准确认定，依法严惩。

5. 利用信息网络威胁他人，强迫交易，情节严重的，依照刑法第二百二十六条的规定，以强迫交易罪定罪处罚。

6. 利用信息网络威胁、要挟他人，索取公私财物，数额较大，或者多次实施上述行为的，依照刑法第二百七十四条的规定，以敲诈勒索罪定罪处罚。

7. 利用信息网络辱骂、恐吓他人，情节恶劣，破坏社会秩序的，依照刑法第二百九十三条第一款第二项的规定，以寻衅滋事罪定罪处罚。

编造虚假信息，或者明知是编造的虚假信息，在信息网络上散布，或者组织、指使人员在信息网络上散布，起哄闹事，造成公共秩序严重混乱的，依照刑法第二百九十三条第一款第四项的规定，以寻衅滋事罪定罪处罚。

8. 侦办利用信息网络实施的强迫交易、敲诈勒索等非法敛财类案件，确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数以及涉案资金数额等。

三、准确认定利用信息网络实施犯罪的黑恶势力

9. 利用信息网络实施违法犯罪活动，符合刑法、《指导意见》以及最高人民法院、最高人民检察院、公安部、司法部《关于办理恶势力刑事案件若干问题的意见》等规定的恶

势力、恶势力犯罪集团、黑社会性质组织特征和认定标准的，应当依法认定为恶势力、恶势力犯罪集团、黑社会性质组织。

认定利用信息网络实施违法犯罪活动的黑社会性质组织时，应当依照刑法第二百九十四条第五款规定的“四个特征”进行综合审查判断，分析“四个特征”相互间的内在联系，根据在网络空间和现实社会中实施违法犯罪活动对公民人身、财产、民主权利和经济、社会生活秩序所造成的危害，准确评价，依法予以认定。

10. 认定利用信息网络实施违法犯罪的黑恶势力组织特征，要从违法犯罪的起因、目的，以及组织、策划、指挥、参与人员是否相对固定，组织形成后是否持续进行犯罪活动、是否有明确的职责分工、行为规范、利益分配机制等方面综合判断。利用信息网络实施违法犯罪的黑恶势力组织成员之间一般通过即时通讯工具、通讯群组、电子邮件、网盘等信息网络方式联络，对部分组织成员通过信息网络方式联络实施黑恶势力违法犯罪活动，即使相互未见面、彼此不熟识，不影响对组织特征的认定。

11. 利用信息网络有组织地通过实施违法犯罪活动或者其他手段获取一定数量的经济利益，用于违法犯罪活动或者支持该组织生存、发展的，应当认定为符合刑法第二百九十四条第五款第二项规定的黑社会性质组织经济特征。

12. 通过线上线下相结合的方式，有组织地多次利用信息网络实施违法犯罪活动，侵犯不特定多人的人身权利、民主权利、财产权利，破坏经济秩序、社会秩序的，应当认定为符合刑法第二百九十四条第五款第三项规定的黑社会性质组织行为特征。单纯通过线上方式实施的违法犯罪活动，且不具有为非作恶、欺压残害群众特征的，一般不应作为黑社会性质组织行为特征的认定依据。

13. 对利用信息网络实施黑恶势力犯罪非法控制和影响的“一定区域或者行业”，应当结合危害行为发生地或者危害行业的相对集中程度，以及犯罪嫌疑人、被告人在网络空间和现实社会中的控制和影响程度综合判断。虽然危害行为发生地、危害的行业比较分散，但涉案犯罪组织利用信息网络多次实施强迫交易、寻衅滋事、敲诈勒索等违法犯罪活动，在网络空间和现实社会造成重大影响，严重破坏经济、社会生活秩序的，应当认定为“在一定区域或者行业内，形成非法控制或者重大影响”。

四、利用信息网络实施黑恶势力犯罪案件管辖

14. 利用信息网络实施的黑恶势力犯罪案件管辖依照《关于办理黑社会性质组织犯罪

案件若干问题的规定》和《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》的有关规定确定，坚持以犯罪地管辖为主、被告人居住地管辖为辅的原则。

15. 公安机关可以依法对利用信息网络实施的黑恶势力犯罪相关案件并案侦查或者指定下级公安机关管辖，并案侦查或者由上级公安机关指定管辖的公安机关应当全面调查收集能够证明黑恶势力犯罪事实的证据，各涉案地公安机关应当积极配合。并案侦查或者由上级公安机关指定管辖的案件，需要提请批准逮捕、移送审查起诉、提起公诉的，由立案侦查的公安机关所在地的人民检察院、人民法院受理。

16. 人民检察院对于公安机关提请批准逮捕、移送审查起诉的利用信息网络实施的黑恶势力犯罪案件,人民法院对于已进入审判程序的利用信息网络实施的黑恶势力犯罪案件，被告人及其辩护人提出的管辖异议成立，或者办案单位发现没有管辖权的，受案人民检察院、人民法院经审查，可以依法报请与有管辖权的人民检察院、人民法院共同的上级人民检察院、人民法院指定管辖，不再自行移交。对于在审查批准逮捕阶段，上级检察机关已经指定管辖的案件，审查起诉工作由同一人民检察院受理。人民检察院、人民法院认为应当分案起诉、审理的，可以依法分案处理。

17. 公安机关指定下级公安机关办理利用信息网络实施的黑恶势力犯罪案件的，应当同时抄送同级人民检察院、人民法院。人民检察院认为需要依法指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。

18. 本意见自 2019 年 10 月 21 日起施行。