贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见

网络安全等级保护制度和关键信息基础设施安全保护制度是党中央有关文件和《网络安全法》确定的基本制度。近年来，各单位、各部门按照中央网络安全政策要求和《网络安全法》等法律法规规定，全面加强网络安全工作，有力保障了国家关键信息基础设施、重要网络和数据安全。但随着信息技术飞速发展，网络安全工作仍面临一些新形势、新任务和新挑战。为深入贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度，健全完善国家网络安全综合防控体系，有效防范网络安全威胁，有力处置网络安全事件，严厉打击危害网络安全的违法犯罪活动，切实保障国家网络安全，特制定以下指导意见。

一、指导思想、基本原则和工作目标

（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，按照党中央、国务院决策部署，以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划，以贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度为基础，以保护关键信息基础设施、重要网络和数据安全为重点，全面加强网络安全防范管理、监测预警、应

急处置、侦查打击、情报信息等各项工作，及时监测、处置网络安全风险、威胁和网络安全突发事件，保护关键信息基础设施、重要网络和数据免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，切实提高网络安全保护能力，积极构建国家网络安全综合防控体系，切实维护国家网络空间主权、国家安全和社会公共利益，保护人民群众的合法权益，保障和促进经济社会信息化健康发展。

（二）基本原则

坚持分等级保护、突出重点。根据网络（包含网络设施、信息系统、数据资源等）在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级（含第三级、下同）以上网络的安全。

坚持积极防御、综合防护。按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

坚持依法保护、形成合力。依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门（含监管部门，下同）依法履行本行业网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

（三）工作目标

网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，网络安全保护良好生态基本建立，国家网络安全综合防护能力和水平显著提升。

关键信息基础设施安全保护制度建立实施。关键信息基础设施底数清晰，安全保护机构健全、职责明确、保障有力。在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强。

网络安全监测预警和应急处置能力显著提升。跨行业、跨部门、跨地区的立体化网络安全监测体系和网络安全保护

平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范、遏制和处置。

网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导和侦查打击等能力显著提升，“打防管控”一体化的网络安全综合防控体系基本形成。

二、深入贯彻实施国家网络安全等级保护制度

按照国家网络安全等级保护制度要求，各单位、各部门在公安机关指导监督下，认真组织、深入开展网络安全等级保护工作，建立良好的网络安全保护生态，切实履行主体责任，全面提升网络安全保护能力。

（一）**深化网络定级备案工作**。网络运营者应全面梳理本单位各类网络，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，科学确定网络的安全保护等级，对第二级以上网络依法向公安机关备案，并向行业主管部门报备。对新建网络，应在规划设计阶段确

定安全保护等级。公安机关对网络运营者提交的备案材料和网络的安全保护等级进行审核，对定级结果合理、备案材料符合要求的，及时出具网络安全等级保护备案证明。行业主管部门可以依据《网络安全等级保护定级指南》国家标准，结合行业特点制定行业网络安全等级保护定级指导意见。

（二）**定期开展网络安全等级测评**。网络运营者应依据有关标准规范，对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患。第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。网络运营者在开展测评服务过程中要与测评机构签署安全保密协议，并对测评过程进行监督管理。公安机关要加强对本地等级测评机构的监督管理，建立测评人员背景审查和人员审核制度，确保等级测评过程客观、公正、安全。

（三）**科学开展安全建设整改**。网络运营者应在网络建设和运营过程中，同步规划、同步建设、同步使用有关网络安全保护措施。应依据《网络安全等级保护基本要求》《网络安全等级保护安全设计技术要求》等国家标准，在现有安全保护措施的基础上，全面梳理分析安全保护需求，并结合等级测评过程中发现的问题隐患，按照“一个中心（安全管理

中心）、三重防护（安全通信网络、安全区域边界、安全计算环境）”的要求，认真开展网络安全建设和整改加固，全面落实安全保护技术措施。网络运营者可将网络迁移上云，或将网络安全服务外包，充分利用云服务商和网络安全服务商提升网络安全保护能力和水平。应全面加强网络安全管理，建立完善人员管理、教育培训、系统安全建设和运维等管理制度，加强机房、设备和介质安全管理，强化重要数据和个人信息保护，制定操作规范和工作流程，加强日常监督和考核，确保各项管理措施有效落实。

（四）**强化安全责任落实**。行业主管部门、网络运营者应依据《网络安全法》等法律法规和有关政策要求，按照“谁主管谁负责、谁运营谁负责”的原则，厘清网络安全保护边界，明确安全保护工作责任，建立网络安全等级保护工作责任制，落实责任追究制度，作到“守土有责、守土尽责”。网络运营者要定期组织专门力量开展网络安全自查和检测评估，行业主管部门要组织风险评估，及时发现网络安全隐患和薄弱环节并予以整改，不断提高网络安全保护能力和水平。

（五）**加强供应链安全管理**。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网

远程运维的，应进行评估论证，并采取相应的管控措施。网络运营者应采购、使用符合国家法律法规和有关标准规范要求的网络产品及服务，第三级以上网络运营者应积极应用安全可信的网络产品及服务。

（六）**落实密码安全防护要求**。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

三、建立并实施关键信息基础设施安全保护制度

公安机关指导监督关键信息基础设施安全保护工作。各单位、各部门应加强关键信息基础设施安全的法律体系、政策体系、标准体系、保护体系、保卫体系和保障体系建设，建立并实施关键信息基础设施安全保护制度，在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。

（一）**组织认定关键信息基础设施**。根据党中央和公安部有关规定，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、国防科技工业等重要行业和领域

的主管、监管部门（以下统称保护工作部门）应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。保护工作部门根据认定规则负责组织认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部。应将符合认定条件的基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象纳入关键信息基础设施。关键信息基础设施清单实行动态调整机制，有关网络设施、信息系统发生较大变化，可能影响其认定结果的，运营者应及时将相关情况报告保护工作部门，保护工作部门应组织重新认定，将认定结果通知运营者，并报公安部。

（二）明确关键信息基础设施安全保护工作职能分工。公安部负责关键信息基础设施安全保护工作的顶层设计和规划部署，会同相关部门健全完善关键信息基础设施安全保护制度体系。保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，根据国家网络安全法律法规和有关标准规范要求，制定并实施本行业、本领域关键信息基础设施安全总体规划和安全防护策略，落实本行业、本领域网络安全指导监督责任。关键信息基础设施运营者负责设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

（三）**落实关键信息基础设施重点防护措施**。关键信息基础设施运营者应依据网络安全等级保护标准开展安全建设并进行等级测评，发现问题和风险隐患要及时整改；依据关键信息基础设施安全保护标准，加强安全保护和保障，并进行安全检测评估。要梳理网络资产，建立资产档案，强化核心岗位人员管理、整体防护、监测预警、应急处置、数据保护等重点保护措施，合理分区分域，收敛互联网暴露面，加强网络攻击威胁管控，强化纵深防御，积极利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的网络安全保护体系，不断提升关键信息基础设施内生安全、主动免疫和主动防御能力。有条件的运营者应组建自己的安全服务机构，承担关键信息基础设施安全保护任务，也可通过迁移上云或购买安全服务等方式，提高网络安全专业化、集约化保障能力。

（四）**加强重要数据和个人信息保护**。运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施，切实保护重要数据全生命周期安全。运营者在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，应当遵守有关规定并进行安全评估。

（五）**强化核心岗位人员和产品服务的安全管理**。要对专门安全管理机构的负责人和关键岗位人员进行安全背景审查，加强管理。要对关键信息基础设施设计、建设、运行、维护等服务实施安全管理，采购安全可信的网络产品和服务，确保供应链安全。当采购产品和服务可能影响国家安全的，应按照国家有关规定通过安全审查。公安机关加强对关键信息基础设施安全服务机构的安全管理，为运营者开展安全保护工作提供支持。

四、加强网络安全保护工作协作配合

行业主管部门、网络运营者与公安机关要密切协同，大力开展安全监测、通报预警、应急处置、威胁情报等工作，落实常态化措施，提升应对、处置网络安全突发事件和重大风险防控能力。

（一）**加强网络安全立体化监测体系建设**。各单位、各部门要全面加强网络安全监测，对关键信息基础设施、重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置。要加强网络新技术研究和应用，研究绘制网络空间地理信息图谱（网络地图），实现挂图作战。行业主管部门、网络运营要建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、

指挥调度等工作，并与公安机关有关安全保卫平台对接，形成条块结合、纵横联通、协同联动的综合防控大格局。重点行业、网络运营者和公安机关要建设网络安全监控指挥中心，落实 7x24 小时值班值守制度，建立常态化、实战化的网络安全工作机制。

（二）**加强网络安全信息共享和通报预警**。行业主管部门、网络运营者要依托国家网络与信息安全信息通报机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。第三级以上网络运营者和关键信息基础设施运营者要开展网络安全监测预警和信息通报工作，及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。公安机关要加强网络与信息安全信息通报预警机制建设和力量建设，不断提高网络安全通报预警能力。

（三）**加强网络安全应急处置机制建设**。行业主管部门、网络运营者要按照国家有关要求制定网络安全应急预案，加强网络安全应急力量建设和应急资源储备，与公安机关密切配合，建立网络安全事件报告制度和应急处置机制。关键信息基础设施运营者和第三级以上网络运营者应定期开展应急演练，有效处置网络安全事件，并针对应急演练中发现的

突出问题和漏洞隐患，及时整改加固，完善保护措施。行业主管部门、网络运营者应配合公安机关每年组织开展的网络安全监督检查、比武演习等工作，不断提升安全保护能力和对抗能力。

（四）**加强网络安全事件处置和案件侦办**。关键信息基础设施、第三级以上网络发生重大网络安全威胁和事件时，行业主管部门、网络运营者和公安机关应联合开展处置。电信业务经营者、网络服务提供者应提供支持及协助。网络运营者应配合公安机关打击网络违法犯罪活动；发现违法犯罪线索、重大网络安全威胁和事件时，应及时报告公安机关和有关部门并提供必要协助。

（五）**加强网络安全问题隐患整改督办**。公安机关建立挂牌督办制度，针对网络运营者网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全案事件的，按照规定的权限和程序，会同行业主管部门对相关负责人进行约谈，挂牌督办，并加大监督检查和行政执法力度，依法依规进行行政处罚。网络运营者应按照有关要求采取措施，及时进行整改，消除重大风险隐患。发生重大网络安全案事件的，行业主管部门应组织全行业开展整改整顿。

五、加强网络安全工作各项保障

（一）**加强组织领导**。各单位、各部门要高度重视网络安全等级保护和关键信息基础设施安全保护工作，将其列入重要议事日程，加强统筹领导和规划设计，认真研究解决网络安全机构设置、人员配备、经费投入、安全保护措施建设等重大问题。行业主管部门和网络运营者要明确本单位主要负责人是网络安全的第一责任人，并确定一名领导班子成员分管网络安全工作，成立网络安全专门机构，明确任务分工，一级抓一级，层层抓落实。

（二）**加强经费政策保障**。各单位、各部门要通过现有经费渠道、保障关键信息基础设施、第三级以上网络等开展等级测评、风险评估、密码应用安全性检测、演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运行维护、监督检查、教育培训等经费投入。关键信息基础设施运营者应保障足额的网络安全投入，作出网络安全和信息化有关决策时应有网络安全管理机构人员参与。有关部门要扶持重点网络安全技术产业和项目，支持网络安全技术研究开发和创新应用，推动网络安全产业健康发展。公安机关要会同相关部门组织实施“一带一路”网络安全战略，支持网络安全企业“走出去”， 与有关国家共享中国网络安全保护经验。

（三）**加强考核评价**。各单位、各部门要进一步健全完善网络安全考核评价制度，明确考核指标，组织开展考核。公安机关将网络安全工作纳入社会治安综合治理考核评价

体系，每年组织对各地区网络安全工作进行考核评价，每年评选网络安全等级保护、关键信息基础设施安全保护工作先进单位，并将结果报告党委政府，通报网信部门。

（四）**加强技术攻关**。各单位、各部门要充分调动网络安全企业、科研机构、专家等社会力量积极参与网络安全核心技术攻关，加强网络安全协同协作、互动互补、共治共享和群防群治。公安机关要会同有关部门加强网络安全等级保护和关键信息基础设施安全保护标准制定工作，出台标准应用指南，加强标准宣贯和应用实施，建设试点示范基地，促进我国网络安全产业和企业的健康发展。

（五）**加强人才培养**。各单位、各部门要加强网络安全等级保护和关键信息基础设施安全保护业务交流，通过组织开展比武竞赛等形式，发现选拔高精尖技术人才，建设人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。