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解读

为深入贯彻党中央有关文件精神和《网络安全法》，指导重点行业、部门全面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，近日，公安部制定出台了《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》，进一步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，有力处置重大网络安全事件，切实保障关键信息基础设施、重要网络和数据安全。

网络安全等级保护制度

01 法律政策依据

1994 年，国家规定对计算机信息系统实行安全等级保护

1994 年 2 月 18 日，中华人民共和国国务院令第 147 号发布了《中华人民共和国计算机信息系统安全保护条例》，其中第六条规定：“公安部主管全国计算机信息系统安全保护工作”；第九条规定：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。

2007 年，信息安全等级保护制度正式开始实施

2007 年 6 月 22 日，公安部、国家保密局、国家密码管理局、原国务院信息化工作办公室联合印发了《信息安全等级保护管理办法》（公通字〔2007〕43 号），标志着等级保护制度正式开始实施。

2017 年，网络安全等级保护制度成为网络安全的基本制度

2017 年 6 月 1 日，《网络安全法》正式实施。第二十一条规定，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。

02 基本内容

简单来说，网络安全等级保护是对网络进行分等级保护、分等级监管。有以下几个关键词:

定级。网络运营者对信息网络、信息系统、网络上的数据和信息，按照重要性和遭受损坏后的危害性分成五个安全保护等级，从第一级到第五级，逐级增高。

备案。等级确定后，第二级（含）以上网络到公安机关备案，公安机关对备案材料和定级准确性进行审核，审核合格后颁发备案证明。

建设。备案单位根据网络的安全等级，安全国家标准开展安全建设整改，建设安全设施、落实安全责任、建立和落实网络安全管理制度。

测评。备案单位选择符合国家要求的测评机构开展等级测评。

监督。公安机关对第二级网络进行指导，对第三级、第四级网络定期开展监督、检查。

03 网络安全等级保护制度 2.0 新特征

国家网络安全等级保护制度实施以来，已经成为国家网络安全的基本制度和基本国策。随着经济社会发展和技术进步，等级保护制度已进入2.0时代。

网络安全等级保护制度2.0在1.0的基础上，实现对新技术、新应用安全保护对象和安全保护领域的全覆盖，更加突出技术思维和立体防范，注重全方位主动防御、动态防御、整体防护和精准防护，强化“一个中心，三重防护”的安全保护体系，把云计算、物联网、移动互联、工业控制系统、大数据等相关新技术新应用全部纳入保护范畴。

关键信息基础设施安全保护制度

《网络安全法》第三十一条规定，国家对公共通信和信息服务、能源、交通、水利、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。

习近平总书记强调，“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。”从世界范围来看，各个国家网络安全立法的核心就是保护关键信息基础设施。加强关键信息基础设施安全保护，既是我国网络安全严峻形势的迫切需要，也是切实贯彻国家安全的必然要求。

根据《网络安全法》和中央文件精神，公安机关指导监督关键信息基础设施安全保护工作。我部正建立完善并实施

关键信息基础设施安全保护制度，指导各单位、各部门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，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，全力提升关键信息基础设施安全防护能力。

《指导意见》主要内容介绍

01 确定了指导思想、基本原则和工作目标

《指导意见》以习近平新时代中国特色社会主义思想为指导，以总体国家安全观为统领，认真贯彻实施网络强国战略，全力保护关键信息基础设施、重要网络和数据安全。

《指导意见》的三大原则。坚持分等级保护、突出重点；坚持积极防御、综合防护；坚持依法保护、形成合力。

《指导意见》的四大工作目标。确保网络安全等级保护制度深入贯彻实施，关键信息基础设施安全保护制度建立实施，网络安全监测预警和应急处置能力显著提升，网络安全综合防控体系基本形成。

02 深入贯彻实施国家网络安全等级保护制度

深化网络定级备案工作。全面梳理包括云计算、物联网、新型互联网、大数据、智能制造等新技术应用在内的运营者全部网络情况，科学确定保护等级，依法向公安机关备案。行业主管部门依据《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。

定期开展网络安全等级测评。对已定级备案网络的安全性进行检测评估，第三级以上网络运营者委托符合国家有关规定的等级测评机构每年开展网络安全等级测评。公安机关加强对本地等级测评机构的监督管理，确保等级测评过程客观、公正、安全。

科学开展安全建设整改。运营者在网络建设和运营过程中应同步规划、同步建设、同步使用网络安全保护措施，可通过网络迁移上云或网络安全服务外包方式充分利用网络安全服务商提升网络安全保护能力。

强化安全责任落实。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，建立网络安全等级保护工作责任制。

加强供应链安全管理。加强网络关键人员的安全管理，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。

落实密码安全防护要求。第三级以上网络运营者在网络规划、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

03 建立并实施关键信息基础设施安全保护制度

组织认定。组织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部门和主管、监管部门制定本行业、本领域关键信息基础设施认定规则并报公安部备案。组织认定关键信息基础设施，

及时将认定结果通知相关设施运营者并报公安部。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均应纳入关键信息基础设施。

明确职能分工。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，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。

重点措施。关键信息基础设施运营者组织开展具体工作，开展安全建设和等级测评，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，积极利用新技术开展网络安全保护。

数据和个人信息保护。加强重要数据和个人信息保护，在境内运营中收集和产生的个人信息和重要数据在境内存储。

核心岗位人员和产品服务。强化核心岗位人员和产品服务的安全管理，采购安全可信的网络产品和服务，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，确保供应链安全。

04 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密切协同。

加强网络安全立体化监测体系建设，对关键信息基础设施、重要网络等开展实时监测。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）。行业主管部门、网络运营建设本行业、本单位的网络安全保护业务平台，建设平台智慧大脑，与公安机关平台对接，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建设网络安全监控指挥中心，建立常态化、实战化的网络安全工作机制。

加强网络安全信息共享和通报预警。依托国家网络与信息安全信息通报机制，加强各行业、各部门网络安全信息通报能力建设。

加强网络安全应急处置机制建设，定期开展应急演练，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。

加强网络安全事件处置和案件侦办和行政执法，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、发生重大网络安全案事件的挂牌督办。

05 加强网络安全工作各项保障

加强组织领导，将网络安全等级保护和关键信息基础设施安全保护工作列入各部门重要议事日程，研究解决网络安全机构、人员、经费、建设等重大问题，明确本单位主要负责人是网络安全的第一责任人，成立网络安全专门机构抓落实。

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。

健全完善网络安全考核评价制度，将网络安全工作纳入考核评价体系。

加强技术攻关，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。加强网络安全等级保护和关键信息基础设施安全保护标准制定工作，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。

加强人才培养，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。