郭启全：《网络安全等级保护条例（征求意见稿）》解读

贯彻落实网络安全法 推进完善等级保护制度

经过二十多年的发展，我国于 1994 年确立的计算机信息系统实行安全等级保护制度逐渐发展成熟，有力地保障了国家信息安全。2017 年 6 月 1 日开始实施的《中华人民共和国网络安全法》，明确将国家网络安全等级保护制度上升为法律要求。至此，我国等级保护制度在逐渐成熟经验的基础上继续发展。《网络安全等级保护条例（征求意见稿）》的颁布和征求意见，既是健全完善相关法律规范体系的需要，也为解决等级保护现实问题提供契机，成为等级保护创新发展的驱动力。

郭启全

公安部网络安全保卫局

总工程师

为深入推进实施网络安全等级保护制度，保障国家网络空间安全和关键信息基础设施安全，按照中央指示精神，公安部会同中共中央网络安全和信息化委员会办公室（以下简称中央网

信办）、国家保密局、国家密码管理局，在总结十几年全国范围开展网络安全等级保护工作经验的基础上，联合起草了《网络安全等级保护条例（征求意见稿）》（以下简称《条例》）。

一、制定《条例》的必要性

（一）是贯彻落实《网络安全法》，健全完善我国网络安全保障工作法律规范体系的需要

近年来，世界主要国家将网络安全作为谋求战略优势的新抓手，对内不断加强顶层设计和能力建设，对外抢抓网络空间控制权、规则制定权和话语权，世界大国网络空间博弈加剧，网络问题已成为大国互动的新焦点、大国战略关系走向的重大课题。我国网络安全形势更是严峻复杂，面临前所未有的威胁、风险和挑战，并存在许多突出的问题和困难。在这种形势下，亟需健全完善我国的网络安全法律体系，为我国网络安全等级保护制度的实施提供法律保障。《网络安全法》明确规定国家实行网络安全等级保护制度，标志着网络安全等级保护制度从1994 年国务院条例（第 147 号令）上升为国家法律要求，标志着我国实施十年之久的信息安全等级保护制度进入新时代、新阶段，标志着以保护国家关键信息基础设施和大数据安全为重点的网络安全等级保护制度将进一步健全完善并依法全面推进实施。以“建设网络强国”为战略目标，以发展需求为牵引，以安全问题为导向，及时制定出台《条例》十分必要、紧迫，这是构建全新网络安全等级保护制度体系、保障关键信息基础设施和大数据安全、依法维护我国网络空间安全的重要举措。

（二）是落实网络安全等级保护制度要求，构建国家网络安全基本制度、基本国策的需要

近年来，有关法规和系列政策文件明确要求，落实网络安全等级保护制度要求，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，不断健全完善网络安全等级保护制度体系。网络安全等级保护是当今发达国家保护关键信息基础设施、保障信息安全的通行做法，也是我国多年来网络安全工作实践和经验的总结。开展网络安全等级保护工作的主要目的就是要保护国家关键信息基础设施安全、维护国家安全，这是一项事关国家安全、社会稳定、国家利益的重要决策部署。十多年来，在党中央的坚强领导下，在有关部门、专家、企业的大力支持下，公安部根据法律授权，会同中央网信办、国家保密局和国家密码管理局，在全国范围内组织开展基础调查、等级保护试点、信息系统定级备案、安全建设整改、等级测评、网络安全大检查等工作，创造性地构建并实施了网络安全等级保护制度，确立了具有中国特色的国家网络安全基本制度和基本国策，全面促进了国家网络安全工作体系化，有力促进了我国网络安全工作法制化、规范化和标准化，全力提升了国家关键信息基础设施安全保护能力。同时，公安部会同国家保密局、国家密码管理局、国资委、国家发改委、财政部、教育部等部门出台了一系列政策文件，逐步构建网络安全等级保护工作的政策体系，组织制定了网络安全等级保护工作需要的一系列标准，形成了网络安全等级保护标准体系，为指导各地区、各部门开展等级保护工作提供了政策保障和标准保障。网络安全等级保护制度业已成为国家网络安全的基本制度、基本策略和基本方法，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。因此，有必要将这一基础性制度通过行政法规的形式固定下来，把多年来网络安全工作中行之有效的方法和措施固化下来，确保《网络安全法》规定的网络安全基本制度得以有效实施。

（三）是应对日益严峻的网络安全形势，解决网络安全突出问题的现实需要

近年来网络安全形势越来越严峻，网络安全事件（案件）频发，面临境内外的网络攻击威胁也越来越大。从公安机关开展网络安全事件处置，以及打击黑客攻击类网络违法犯罪案件的情况看，有超过 80%的网络安全事件（案件）都是因为网络运营者自身安全保护重视不够，基本安全保护措施不落实等原因造成。目前，网络安全等级保护制度实施的主要依据是 2007 年公安部、国家保密局、国家密码管理局、原国务院信息办联合出台的《信息安全等级保护管理办法》（公通字〔2007〕43 号），属于规范性文件，不具备法律效力，适用范围仅限政府部门内部，约束性差，导致公安机关、保密部门、密码管理部门的监督管理力度不大，

对不落实等级保护制度要求的单位无法进行行政处罚。因此，需要以《网络安全法》和《网络安全等级保护条例》共同支撑国家网络安全等级保护制度的全面有效地贯彻落实。

二、《条例》内容解读

针对网络安全等级保护制度等立法层级不高、执行强制性差，公安机关等网络安全职能部门行政执法支撑不足等问题，中央领导同志就网络安全等级保护立法工作多次作出批示，要求加强等级保护立法工作，健全完善以保护国家关键信息基础设施安全为重点的网络安全等级保护制度。根据政策文件和中央领导指示精神，为落实《网络安全法》的规定，公安部牵头《条例》起草工作，并成立了起草工作专班。《条例》起草工作专班经过深入调研、广泛座谈、多轮研讨、全面征求意见建议、反复修改完善，形成了《条例》（征求意见稿）。《条例》共八章七十三条。按照工作惯例和工作职责，其中第三章“涉密网络的安全保护”由国家保密局负责起草，第四章“密码管理”由国家密码管理局负责起草。《条例》主要内容如下：

（一）关于总则

总结十多年的实践，总则中对立法依据、适用范围、原则和保护重点、职责分工等做了明确规定。国家实行网络安全等级保护制度，对网络实施分等级保护、分等级监管，《条例》适用于中华人民共和国境内建设、运营、维护、使用网络开展网络安全等级保护工作以及监督管理，个人及家庭自用的网络除外。《条例》中延用《网络安全法》中网络的概念：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规则和程序对数据信息进行收集、存储、传输、交换、处理的信息网络、信息系统和数据资源。网络安全等级保护制度在十多年成功实践的基础上，结合当前信息技术的发展和形势需要，不断与时俱进、健全完善。一是将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等重点措施纳入等级保护制度并实施。二是将网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网、工控系统、公众服务平台、互联网企业等全部纳入等级保护监管。网络安全等级保护工作重点保护的是涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。同时，总则中强调了网络安全的三同步原则，即网络运营者在网络建设过程中，应当同步规划、同步建设、同步运行网络安全保护、保密和密码保护措施。此外，总则中还规定了中央网信办、公安部门、保密行政管理部门、国家密码管理部门以及国务院其他有关部门、行业主管部门在网络安全等级保护工作中的职责。

（二）关于支持与保障

《条例》第二章中明确了国家和政府落实网络安全等级保护制度的职责任务，重点体现在组织领导、技术支持、保障考核、宣传培训和鼓励创新等方面，从国家层面保障支持等级保护制度的实施和落地，形成自上而下的等级保护工作推进体系。第八条规定国家建立健全网络安全等级保护制度的组织领导体系、技术支持体系和保障体系。各级人民政府和行业主管部门应当将网络安全等级保护制度实施纳入信息化工作总体规划，统筹推进。第九条规定国家建立完善等级保护标准体系。标准化部门和公安、保密、密码部门根据各自职责，组织制定等级保护国家标准、行业标准。在投入和保障方面，各级人民政府鼓励扶持网络安全等级保护重点工程和项目，支持网络安全等级保护技术的研究开发和应用。在技术支持方面，国家建设网络安全等级保护专家队伍和等级测评、安全建设、应急处置等技术支持体系，为网络安全等级保护制度提供支撑。

（三）关于网络的安全保护

《条例》第三章中规定了网络安全等级保护制度体系的基本框架、具体内容、要求和相关主体的责任义务。

一是明确了网络运营者依法落实网络安全等级保护制度。按照《条例》规定开展网络定级、备案、测评、整改、自查工作，公安机关对网络分级监督管理的职责及其在备案审核、服务机构管理、事件调查、执法检查中的职责。《条例》中的内容与《关键信息基础设施保护条例（征求意见稿）》有关内容进行了协调衔接。

二是规定了网络的定级和备案要求。根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级（如表）。

网络运营者或主管部门应参考 GA/T 1389-2017《信息安全技术 网络安全等级保护定级指南》的要求，梳理出定级对象并合理确定其所属网络的安全保护等级、确定其安全责任单位和具体责任人。定级时应当注意以下几个方面：一是网络运营者应当在规划设计阶段确定网络的安全保护等级；当网络功能、服务范围、服务对象和处理的数据等发生重大变化时，网络运营者应当依法变更网络的安全保护等级；网络定级应按照网络运营者拟定网络等级、专家评审、主管部门核准、公安机关审核的流程进行。对于基础网络、云计算平台和大数据平台等起支撑作用的网络系统，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。原则上大数据的安全等级不低于第三级。

三是《条例》在《网络安全法》规定的网络运营者安全保护义务的基础上，对不同安全保护等级网络的运营者的安全保护义务做了明确、细化的要求。第二十条规定了网络运营者应当依法履行的 11 项一般性安全保护义务，包括落实责任制，建立并落实安全管理和技术保护制度，制定并落实机房安全管理、设备和介质安全管理等操作规范和工作流程，落实身份识别、防范恶意代码感染传播和网络入侵攻击的管理和技术措施，落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，相关网络日志留存以及落实数据分类、重要数据备份和加密、个人信息保护措施，对网络中发生的案事件应当向属地公安机关报告等网络安全保护义务。第三级以上网络的运营者，除履行上述网络安全保护义务之外，根据第二十二条规定，还应当履行的其他 8 项安全保护义务包括：强化网络安全管理机构的职责，重大事项逐级审批，网络安全管理负责人和关键岗位的人员安全背景审查，采取网络安全态势感知监测预警措施进行动态监测分析以及落实备份和恢复措施、定期开展等级测评等网络安全保护义务，突出强化了国家对关键信息基础设施和其他重要网络的重点保护和管理。

四是规定了第三级以上网络运营者在开展技术维护、监测预警、信息通报、应急处置以及数据信息安全等工作时应当履行的责任义务。同时，《条例》中就测评服务、安全监测、运维、数据应用等其安全服务机构管理提出了明确的管理要求，提出了新技术新应用的风险管控规定。

（四）关于涉密网络系统的安全保护

《条例》第四章中提出了涉密网络安全保密总体要求，以及涉密网络分级保护要求和涉密网络使用管理要求，明确了涉密网络全过程管理，规定了涉密网络密级确定、方案论证、建设实施、测评审查、风险评估、重大变化以及废止等环节的保密管理要求。

（五）关于密码管理

《条例》第五章中明确提出了密码配备使用、管理和应用安全性评估的有关要求，对网络的密码保护做出规定。其中，对涉密网络，明确密码检测、装备、采购、使用以及系统设计、运行维护、日常管理等要求；对非涉及国家秘密网络、第三级以上网络提出密码保护要求，明确规定网络运营者应在网络规划、建设和运行阶段委托专业测评机构开展密码应用安全性评估，并对评估结果备案提出了要求。

（六）关于保障和监督管理

为深入推进实施网络安全等级保护制度，《条例》第六章规定了公安机关、行业主管（监管）部门等在网络安全监督管理中的职责和监管要求，就重大隐患处置、安全服务机构监管、事件调查以及保密、密码的监督管理等分别做了明确规定，提出了网络运营者和技术支持单位应履行的执法协助义务。

三、处理好网络安全等级保护制度与关键信息基础设施保护的关系

自《网络安全法》发布实施以来，国家网络安全等级保护制度和关键信息基础设施保护的关系问题备受关注。网络安全等级保护制度是我国网络安全保障领域普适性的制度，是关键信息基础设施保护的基础，而关键信息基础设施是网络安全等级保护制度保护的重中之重。网络安全等级保护制度和关键信息基础设施保护是网络安全的两个重要方面，不可分割。关键信息基础设施运营单位须按照网络安全等级保护制度要求，开展关键信息基础设施定级备案、等级测评、安全建设整改、安全检查等强制性、规定性工作。网络运营者应当在安全保护等级为第三级（含）以上网络中确定关键信息基础设施，即认定为关键信息基础设施的，其安全保护等级不低于第三级。网信、公安、保密、密码等部门要落实关键信息基础设施保护监管责任，关键信息基础设施网络运营单位和保护工作部门要落实主体责任。各相关单位、部门各司其职、各负其责，充分发挥职能作用，调动国家资源力量，保障关键信息基础设施安全。