能源局关于印发《电力行业网络安全等级保护管理办法》的通知

国能发安全规〔2022〕101号

各省（自治区、直辖市）能源局，有关省（自治区、直辖市）及新疆生产建设兵团发展改革委、工业和信息化主管部门，北京市城市管理委，各派出机构，全国电力安全生产委员会各企业成员单位，有关电力企业：

为深入贯彻习近平总书记关于网络强国的重要思想，规范电力行业网络安全等级保护管理，提高电力行业网络安全保障能力和水平，国家能源局对《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318号）进行了修订。现将修订后的《电力行业网络安全等级保护管理办法》印发你们，请遵照执行。

能　源　局

2022年11月16日

电力行业网络安全等级保护管理办法

第一章　总　　则

第一条　为规范电力行业网络安全等级保护管理，提高电力行业网络安全保障能力和水平，维护国家安全、社会稳定和公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国计算机信息系统安全保护条例》、《关键信息基础设施安全保护条例》、《信息安全等级保护管理办法》等法律法规和规范性文件，制定本办法。

第二条　电力企业在中华人民共和国境内建设、运营、维护、使用网络（除核安全外），开展网络安全等级保护工作，适用本办法。

本办法所称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，包括电力监控系统、管理信息系统及通信网络设施。

本办法不适用于涉及国家秘密的网络。涉及国家秘密的网络应当按照国家保密工作部门有关涉密信息系统分级保护的管理规定和技术标准，结合网络实际情况进行管理。

第三条　国家能源局根据国家网络安全等级保护政策法规和技术标准要求，结合行业实际，组织制定适用于电力行业的网络安全等级保护管理规范和技术标准，对电力行业网络安全等级保护工作的实施进行指导和监督管理。国家能源局各派出机构根据国家能源局授权，对本辖区电力企业网络安全等级保护工作的实施进行监督管理。

电力企业依照国家和电力行业相关法律法规和规范性文件，履行网络安全等级保护的义务和责任。

第二章　等级划分与保护

第四条　根据电力行业网络在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、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、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素，电力行业网络划分为五个安全保护等级：

第一级，受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益。

第二级，受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全。

第三级，受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害。

第四级，受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害。

第五级，受到破坏后，会对国家安全造成特别严重危害。

第五条　电力行业网络安全等级保护坚持分等级保护、突出重点、积极防御、综合防范的原则。

第三章　等级保护的实施与管理

第六条　国家能源局根据《信息安全技术网络安全等级保护定级指南》（GB/T 22240）等国家标准规范，结合电力行业网络特点，制定电力行业网络安全等级保护定级指南，指导电力行业网络安全等级保护定级工作。

第七条　电力企业应当在网络规划设计阶段，依据《信息安全技术网络安全等级保护定级指南》（GB/T 22240）等国家标准规范和电力行业网络安全等级保护定级指南，确定定级对象（网络）及其安全保护等级，并在网络功能、服务范围、服务对象和处理的数据等发生重大变化时，及时申请变更其安全保护等级。

对拟定为第二级及以上的网络，电力企业应当组织网络安全专家进行定级评审。其中，拟定为第四级及以上的网络，还应当由国家能源局统一组织国家网络安全等级保护专家进行定级评审。

第八条　全国电力安全生产委员会企业成员单位汇总集团总部拟定为第二级及以上网络的定级结果和专家评审意见，报国家能源局审核。各区域（省）内的电力企业汇总本单位拟定为第二级及以上网络的定级结果，报国家能源局派出机构审核。

第九条　电力企业办理网络安全等级保护定级审核手续时，应当提交《电力行业网络安全等级保护定级审核表》（详见附件），含各定级对象的定级报告及专家评审意见。

国家能源局或其派出机构应当在收到审核材料之日起30日内反馈审核意见。

第十条　电力企业应当在收到国家能源局或其派出机构审核意见后，按照有关规定向公安机关备案并按照第八条规定的定级审核权限向国家能源局或其派出机构报告定级备案结果。

第十一条　电力企业应当采购、使用符合国家法律法规和有关标准规范要求且满足网络安全等级保护需求的网络产品和服务。

对于电力监控系统，应当按照电力监控系统安全防护有关要求，采购和使用电力专用横向单向安全隔离装置、电力专用纵向加密认证装置或者加密认证网关等设备设施；在设备选型及配置时，禁止选用经国家能源局通报存在漏洞和风险的系统及设备，对已经投入运行的系统及设备应及时整改并加强运行管理和安全防护。

采购网络产品和服务，影响或可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第十二条　电力企业在网络规划、建设、运营过程中，应当遵循同步规划、同步建设、同步使用的原则，并按照该网络的安全保护等级要求，建设网络安全设备设施，制定并落实安全管理制度，健全网络安全防护体系。

第十三条　网络建设完成后，电力企业应当依据国家和行业有关标准或规范要求，定期对网络安全等级保护状况开展网络安全等级保护测评。第二级网络应当每两年进行一次等级保护测评，第三级及以上网络应当每年进行一次等级保护测评。新建的第三级及以上网络应当在通过等级保护测评后投入运行。

电力监控系统网络安全等级保护测评工作应当与电力监控系统安全防护评估、关键信息基础设施网络安全检测评估、商用密码应用安全性评估工作相衔接，避免重复测评。

电力企业应当定期对网络安全状况、安全保护制度及措施的落实情况进行自查。第二级电力监控系统应当每两年至少进行一次自查，第三级及以上网络应当每年至少进行一次自查。

电力企业应当对自查和等级保护测评中发现的安全风险隐患，制定整改方案，并开展安全建设整改。

电力企业应当要求网络安全等级保护测评机构（以下简称测评机构）组织专家对第三级及以上网络的等级保护测评报告进行评审，并随测评报告提交专家评审意见。

第十四条　电力企业应当按照第八条规定的定级审核权限，每年向国家能源局或其派出机构报告网络安全等级保护工作情况，包括网络安全等级保护定级备案、等级保护测评、安全建设整改、安全自查等情况。

第十五条　国家能源局及其派出机构结合关键信息基础设施网络安全检查，定期组织对运营有第三级及以上网络的电力企业开展抽查。开展网络安全检查时应当加强协同配合和信息沟通，避免不必要的检查和交叉重复检查。

检查事项主要包括：

（一）网络安全等级保护定级工作开展情况，包括定级评审、审核、备案及根据网络安全需求变化调整定级等情况；

（二）电力企业网络安全管理制度、措施的落实情况；

（三）电力企业对网络安全状况的自查情况；

（四）网络安全等级保护测评工作开展情况；

（五）网络安全产品使用情况；

（六）网络安全建设整改情况；

（七）备案材料与电力企业及其网络的符合情况；

（八）其他应当进行监督检查的事项。

第十六条　电力企业应当接受国家能源局及其派出机构的安全监督、检查、指导，根据需要如实提供下列有关网络安全等级保护的信息资料及数据文件：

（一）网络安全等级保护定级备案事项变更情况；
（二）网络安全组织、人员、岗位职责的变动情况；
（三）网络安全管理制度、措施变更情况；
（四）网络运行状况记录；
（五）电力企业对网络安全状况的自查记录；
（六）测评机构出具的网络安全等级保护测评报告；
（七）网络安全产品使用的变更情况；
（八）网络安全事件应急预案，网络安全事件应急处置结果报告；
（九）网络数据容灾备份情况；
（十）网络安全建设、整改结果报告；
（十一）其他需要提供的材料。

第十七条　针对网络安全检查发现的问题，电力企业应当按照网络安全等级保护管理规范和技术标准组织整改。必要时，国家能源局及其派出机构可对整改情况进行抽查。

第十八条　电力企业选择测评机构进行网络安全等级保护测评时，应当遵循以下要求：

（一）测评机构应当获得由国家认证认可委员会批准的认证机构发放的《网络安全等级测评与检测评估机构服务认证证书》（以下简称测评机构服务认证证书）。

（二）从事电力监控系统网络安全等级保护测评的机构应当熟悉电力监控系统网络安全管理和技术防护要求，具备相应的服务能力和经验。从事电力监控系统第二级网络等级保护测评的机构应当具备近2年内30套以上工业控制系统等级保护测评或风险评估服务经验；从事电力监控系统第三级网络等级保护测评的机构应当具备近3年内50套以上电力监控系统等级保护测评或安全防护评估服务经验；从事电力监控系统第四级及以上网络等级保护测评的机构应当具备近5年内90套以上电力监控系统等级保护测评或安全防护评估服务经验。

（三）对属于电力行业关键信息基础设施的网络，选择测评机构时应当保证其安全可信，必要时可要求测评机构及其主要负责人、技术骨干提供无犯罪记录证明等材料。

（四）不得委托近3年内被国家能源局通报有本办法规定不良行为，或被认证机构通报取消或暂停使用测评机构服务认证证书，或被国家网络安全等级保护工作主管部门、行业协会通报暂停开展等级保护测评业务并处于整改期内的测评机构。

（五）电力企业应当采取签署保密协议、开展安全保密培训和现场监督等措施，加强对测评机构、测评人员和测评过程的安全保密管理，避免发生失泄密事件。

第十九条　国家能源局及其派出机构在开展电力企业网络安全检查工作时，可同步对测评机构开展的测评工作情况进行监督检查。

第二十条　国家能源局鼓励电力企业按照国家有关要求开展测评机构建设、申请测评机构服务认证，支持电力企业参与制定电力行业网络安全等级保护技术标准。

第四章　网络安全等级保护的密码管理

第二十一条　电力企业采用密码进行等级保护的，应当遵照《中华人民共和国密码法》等有关法律法规和国家密码管理部门制定的网络安全等级保护密码技术标准执行。

第二十二条　电力企业网络安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。运用密码技术进行网络安全等级保护建设与整改时，应当采用商用密码检测、认证机构检测认证合格的商用密码产品和服务。涉及商用密码进口的，还应当符合国家商用密码进口许可有关要求。

第二十三条　电力企业应当按照有关法律法规要求，开展商用密码应用安全性评估工作。

第二十四条　各级密码管理部门对网络安全等级保护工作中密码配备、使用和管理的情况进行检查和安全性评估时，相关电力企业应当积极配合。对于检查和安全性评估发现的问题，应当按照要求及时整改。

第五章　法律责任

第二十五条　电力企业违反国家相关规定及本办法规定，由国家能源局及其派出机构按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，造成严重损害的，由公安机关、密码管理部门依照有关法律、法规予以处理。

第二十六条　有关部门及其工作人员在履行监督管理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

第二十七条　测评机构违反有关法律法规和规范性文件要求，发生以下不良行为时，国家能源局可向国家有关部门、认证机构、行业协会等提出限期整改、取消/暂停使用测评机构服务认证证书等建议，并向电力企业通报相关风险信息：

（一）提供不客观、不公正的等级保护测评服务，出具虚假或不符合实际情况的测评报告，影响等级保护测评的质量和效果；

（二）泄露、出售或者非法向他人提供在服务中知悉的国家秘密、工作秘密、商业秘密、重要数据、个人信息和隐私，非法使用或擅自发布、披露在服务中收集掌握的数据信息和系统漏洞、恶意代码、网络入侵攻击等网络安全信息；

（三）由于测评机构从业人员的因素，导致发生网络安全事件；

（四）未向公安机关报备，测评机构从业人员擅自参加境外组织的网络安全竞赛等活动；

（五）其他危害或可能危害电力生产安全或网络安全的行为。

第六章　附　　则

第二十八条　本办法自发布之日起施行，有效期5年。《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318号）同时废止。

附件：电力行业网络安全等级保护定级审核表（略，详情请登录能源局网站）