国家能源局文件

国能安全〔2014〕318号

国家能源局关于印发《电力行业信息安全等级保护管理办法》的通知

各派出机构，各有关电力企业：

为了进一步加强电力行业信息安全等级保护工作，贯彻落实国家信息安全等级保护要求，国家能源局制定了《电力行业信息安全等级保护管理办法》，现印发你们，请依照执行。

国家能源局

2014年9月22日

电力行业信息安全等级保护管理办法

第一章 总则

第一条 为规范电力行业信息安全等级保护管理，提高电力信息系统安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法》，制定本办法。

第二条 国家能源局根据国家信息安全等级保护管理规范和技术标准要求，督促、检查、指导电力行业信息系统运营、使用单位的信息安全等级保护工作，结合行业实际，组织制定适用于电力行业的信息安全等级保护管理规范和技术标准，组织电力企业对信息系统分等级实行安全保护，对等级保护工作的实施进行监督管理。

国家能源局派出机构根据国家能源局的授权,负责对本辖区电力企业信息系统安全等级保护工作的实施进行监督管理。

第三条 电力信息系统运营、使用单位应当依照本办法及其相关标准规范，履行信息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 电力行业信息安全等级保护坚持自主定级、自主保护的原则。电力信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安

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确定。

第五条 电力信息系统的安全保护等级分为以下四级:

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

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

第六条 电力信息系统运营、使用单位应当分等级对信息系统进行保护，国家能源局及有关信息安全监管部门对其信息安全等级保护工作进行监督管理。

第一级电力信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级电力信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。国家能源局及有关信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。

第三级电力信息系统运营、使用单位应当依据国家有关管理规

范和技术标准进行保护。国家能源局及有关信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。

第四级电力信息系统运营、使用单位应当依据国家有关管理规范、技术标准和业务专门需求进行保护。国家能源局及有关信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

第三章 等级保护的实施与管理

第七条 电力信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》（GB/T 25058-2010）具体实施等级保护工作。电力信息系统运营、使用单位应当依据本办法、《信息系统安全等级保护定级指南》（GB/T 22240-2008）和《电力行业信息系统安全等级保护定级指导意见》确定信息系统的安全保护等级。

第八条 全国电力安全生产委员会成员单位汇总本单位运行、使用的信息系统的定级结果报国家能源局备案。各区域（省）内的电力企业汇总本单位运行、使用的信息系统的定级结果报国家能源局派出机构备案。

第九条 电力信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展电力信息系统安全建设或者改建工作。

第十条 在电力信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）、《电力行业信息系统安全等级保护基本要求》等标准或规范要求，参照《信息系统等级保护安全设计要求》（GB/T25070-2010）、《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全技术 服务器安全技术要求》（GB/T 21028-2007）、《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）等技术标准同步建设符合该等级要求的信息安全设施。

第十一条 电力信息系统运营、使用单位应当参照《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）、《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）、《信息安全技术 信息系统安全等级保护基本要求》（GB/T22239-2008）、《电力行业信息系统安全等级保护基本要求》等标准或规范要求，制定并落实符合本系统安全保护等级要求的安全管理制度。

第十二条 电力信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息安全技术 信息系统安全等级保护测评过程指南》（GB/T 28449-2012）、

《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）、《信息系统安全等级保护测评要求》（GB/T 28448-2012）、《电力行业信息系统安全等级保护基本要求》等标准或规范要求，定期对电力信息系统安全等级状况开展等级测评。电力监控系统信息安全等级测评工作应当与电力监控系统安全防护评估工作同步进行。

电力信息系统运营、使用单位应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第二级生产控制类信息系统和重要生产管理类信息系统应当每两年至少进行一次自查，第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查。

经测评，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。

承担第三级及以上电力信息系统测评任务的测评机构需对测评报告组织专家评审，并将测评报告报国家能源局备案。

第十三条 已运营（运行）的第二级及以上电力信息系统，应当在安全保护等级确定后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

新建第二级以上电力信息系统，应当在投入运行后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

属于全国电力安全生产委员会成员单位的电力集团公司，其跨

省或者全国统一联网运行的电力信息系统，由电力集团公司向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。

第十四条 办理电力信息系统安全保护等级备案手续时，应当填写公安部监制的《信息系统安全等级保护备案表》，第三级及以上信息系统应当同时提供以下材料：

（一）系统拓扑结构及说明；

（二）系统安全组织机构和管理制度；

（三）系统安全保护设施设计实施方案或者改建实施方案；

（四）系统使用的信息安全产品清单及其认证、销售许可证明；

（五）测评后符合系统安全保护等级的技术检测评估报告；

（六）信息系统安全保护等级专家评审意见；

（七）本企业的上级信息安全管理部门对信息系统安全保护等级的意见。

在备案过程中，应当按照公安机关的审核意见，对不符合等级保护要求的备案材料进行纠正后重新备案。

第十五条 国家能源局及其派出机构对第三级及以上电力信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。根据《信息安全等级保护管理办法》，每年应至少组织一次对第三级及以上电力信息系统的检查。

检查事项主要为：

（一）信息系统安全需求是否发生变化，原定保护等级是否准确；

（二）运营、使用单位安全管理制度、措施的落实情况；

（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；

（四）系统安全等级测评是否符合要求；

（五）信息安全产品使用是否符合要求；

（六）信息系统安全整改情况；

（七）备案材料与运营、使用单位、信息系统的符合情况；

（八）其他应当进行监督检查的事项。

第十六条 电力信息系统运营、使用单位应当接受国家能源局及其指定的专门机构的安全监督、检查、指导，如实向国家能源局及其指定的专门机构提供下列有关信息安全保护的信息资料及数据文件：

（一）信息系统备案事项变更情况；

（二）安全组织、人员、岗位职责的变动情况；

（三）信息安全管理制度、措施变更情况；

（四）信息系统运行状况记录；

（五）运营、使用单位及上级部门定期对信息系统安全状况的检查记录；

（六）对信息系统开展等级测评的技术测评报告；

（七）信息安全产品使用的变更情况；

（八）信息安全事件应急预案，信息安全事件应急处置结果报告；

（九）信息系统数据容灾备份情况。

（十）信息系统安全建设、整改结果报告。

第十七条 电力信息系统运营、使用单位应当根据信息安全等级保护工作检查整改通知要求，按照信息安全等级保护管理规范和技术标准进行整改。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 电力信息系统应当选择使用通过国家检测认证的信息安全产品。

第十九条 第二级及以上电力信息系统应当选择符合下列条件的等级保护测评机构进行测评：

（一）在中华人民共和国境内注册成立（港澳台地区除外）；

（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

（三）从事电力信息系统相关检测评估工作两年以上，无违法记录；

（四）工作人员仅限于中国公民；

（五）法人及主要业务、技术人员无犯罪记录；

（六）使用的技术装备、设施应当符合国家对信息安全产品的

要求；

（七）具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

（八）对国家安全、社会秩序、公共利益不构成威胁；

（九）从事电力信息系统测评的技术人员应当通过国家能源局组织的电力系统专业技术培训和考核，开展电力信息系统测评的机构应向国家能源局备案且通过电力测评机构技术能力评估。

第二十条 从事电力信息系统安全等级测评的机构，应当履行下列义务：

（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；

（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；

（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第二十一条 涉及国家秘密的电力信息系统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，结合系统实际情况进行保护。非涉密电力信息系统不得处理国家秘密信息。

第四章 信息安全等级保护的密码管理

第二十二条 电力信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护商用密码管理办法》、《信息安全等级保护商用密码技术要求》等密码管理规定和技术标准。

第二十三条 电力信息系统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。

第二十四条 电力信息系统运营、使用单位采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

第二十五条 电力信息系统运营、使用单位运用密码技术对电力信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准予销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

第二十六条 电力信息系统中采用的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码和密码设备进行评测和监控。

第二十七条 各级密码管理部门对电力信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评时，相关电力企业应当积极配合。对于检查和测评中所反馈的问题，应当按照国家密码管理的相关规定要求及时整改。

第五章 法律责任

第二十八条 第二级及以上电力信息系统运营、使用单位违反国家相关规定及本办法规定，由国家相关部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，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，由相关部门依照有关法律、法规予以处理。

第二十九条 信息安全监管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。

第六章 附 则

第三十条 本办法由国家能源局负责解释。

第三十一条 本办法自发布之日起施行，有效期五年。

抄送：中央网络安全和信息化领导小组办公室，国家发展改革委，公安部（十一局）