公信安〔2018〕765号

关于印发《网络安全等级保护测评机构管理办法》的通知

各省、自治区、直辖市公安厅、局网络安全保卫总队，新疆生产建设兵团公安局网络安全保卫总队:

为进一步加强网络安全等级保护测评机构管理，规范测评行为，提升测评能力和质量，保障国家网络安全等级保护制度深入贯彻实施，我局在近年来工作实践的基础上，组织制定了《网络安全等级保护测评机构管理办法》。现印发各地，请认真贯彻执行。

公安部第十一局

2018年3月23日

网络安全等级保护测评机构管理办法

第一章 总则

第一条 为加强网络安全等级保护测评机构（以下简称“测评机构”）管理，规范测评行为，提高等级测评能力和服务水平，根据《中华人民共和国网络安全法》和网络安全等级保护制度要求，制定本办法。

第二条 等级测评工作，是指测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检测评估的活动。

测评机构，是指依据国家网络安全等级保护制度规定，符合本办法规定的基本条件，经省级以上网络安全等级保护工作领导（协调）小组办公室（以下简称“等保办”）审核推荐，从事等级测评工作的机构。

第三条 测评机构实行推荐目录管理。测评机构由省级以上等保办根据本办法规定，按照统筹规划、合理布局的原则，择优推荐。

第四条 测评机构联合成立测评联盟。测评联盟按照章程和有关测评规范，加强行业自律，提高测评技术能力和服务质量。测评联盟在国家等保办指导下开展工作。

第五条 测评机构应按照国家有关网络安全法律法规规

定和标准规范要求，为用户提供科学、安全、客观、公正的等级测评服务。

第二章　测评机构申请

第六条 申请成为测评机构的单位（以下简称“申请单位”）需向省级以上等保办提出申请。

国家等保办负责受理隶属国家网络安全职能部门和重点行业主管部门的申请，对申请单位进行审核、推荐；监督管理全国测评机构。

省级等保办负责受理本省（区、直辖市）申请单位的申请，对申请单位进行审核、推荐；监督管理其推荐的测评机构。

第七条 申请单位应具备以下基本条件：

（一）在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位;

（二）产权关系明晰，注册资金500万元以上，独立经营核算，无违法违规记录；

（三）从事网络安全服务两年以上，具备一定的网络安全检测评估能力；

（四）法人、主要负责人、测评人员仅限中华人民共和国境内的中国公民，且无犯罪记录；

（五）具有网络安全相关工作经历的技术和管理人员不少于15人，专职渗透测试人员不少于2人，岗位职责清晰，且人员相对稳定；

（六）具有固定的办公场所，配备满足测评业务需要的检测评估工具、实验环境等；

（七）具有完备的安全保密管理、项目管理、质量管理、人员管理、档案管理和培训教育等规章制度；

（八）不涉及网络安全产品开发、销售或信息系统安全集成等可能影响测评结果公正性的业务（自用除外）；

（九）应具备的其他条件。

第八条 申请时，申请单位应向等保办提交以下材料：

（一）网络安全等级保护测评机构推荐申请表；

（二）近两年从事网络安全服务情况以及网络安全服务项目完整文档和相关用户证明；

（三）检测评估工作所需实验环境及测评工具、设备设施情况；

（四）有关管理制度情况；

（五）申请单位及其测评人员基本情况；

（六）应提交的其他材料。

第九条 等保办收到申请材料后，应在10个工作日内组织初审。对符合本办法第七条规定的申请单位，应委托测评联盟对其开展测评能力评估。

测评联盟组织专家，根据标准规范对申请单位开展能力评估，出具测评能力评估报告，并及时将能力评估情况反馈等保办。

能力评估不达标的，等保办应告知申请单位初审未通过。

第十条 初审通过的申请单位，应组织本单位人员参加测评师培训。考试合格的，取得测评师证书。

测评师分为初级、中级和高级。申请单位应至少有15人获得测评师证书，其中高级测评师不少于1人，中级测评师不少于5人。

第十一条 等保办组织专家对人员培训符合要求的申请单位进行复核。复核通过的，颁发《网络安全等级保护测评机构推荐证书》。

第十二条 测评机构实行目录管理，国家等保办编制《全国网络安全等级保护测评机构推荐目录》，并在中国网络安全等级保护网网站发布并及时更新。

省级等保办应及时将本地测评机构推荐情况报国家等保办。

第十三条 省级等保办每年年底根据测评工作需求制定下一年度测评机构推荐计划，并报国家等保办审定。

省级以上等保办受理测评机构申请的时间为每年三月份。

第十四条 测评联盟应组织专家对新推荐测评机构的首个测评项目实施情况进行跟踪评议，并将结果及时报等保办。等保办组织进行综合审查。

第三章　测评机构和测评人员管理

第十五条 测评机构应与被测评单位签署测评服务协议，依据有关标准规范开展测评业务，防范测评风险，客观准确地反映被测评对象的安全保护状况。

测评机构应按照统一模板出具网络安全等级测评报告，并针对被测评网络分别出具等级测评报告。

对第三级以上网络提供等级测评服务的，测评师人数不得少于4名，其中高级测评师、中级测评师应各不少于1名。

第十六条 测评机构应当指定专人管理测评专用章，制定管理规范，不得滥用。

出具等级测评报告时，测评机构应加盖等级测评专用章。未加盖专用章的报告，视为无效。

第十七条 测评师上岗前，测评机构应组织岗前培训；培训合格的，由测评机构配发上岗证，上岗证发放情况应于发放后5个工作日报等保办。测评机构应当对测评师开展等级测评业务情况进行考核，并留存相关记录。

未取得测评师证书和上岗证的，不得参与等级测评项

目。测评师一年内未参与测评活动的，测评联盟应注销其证书。

测评师实行年度注册管理。年审时，测评机构应将本机构测评师情况报等保办注册。测评机构不得采取挂靠或者聘用兼职测评师开展测评业务。

第十八条 测评机构应采取管理和技术措施保护测评活动中相关数据和信息的安全，不得泄露在测评服务中知悉的商业秘密、重要敏感信息和个人信息；未经等保办同意，不得擅自发布、披露在测评服务中收集掌握的网络信息、系统漏洞、恶意代码、网络攻击等信息。

第十九条 测评机构提供测评服务不受地域、行业、领域的限制。测评项目采取登记管理。测评机构在实施测评项目之前，须将测评项目信息及时、准确地填报到网络安全等级保护测评项目登记管理系统（以下简称“项目管理系统”）。

测评机构应于测评项目合同签订后或测评活动实施前5个工作日内，通过项目管理系统填报测评项目基本情况，不得于测评项目完成后进行补录。由于项目实施变更导致已登记信息与实际情况不符的，应及时修改并说明理由。

第二十条 省级以上等保办对测评机构填报的信息应在5个工作日内进行审核确认。逾期未审核确认的，项目管理系统默认审核通过。测评项目填报登记和审核确认的具体要求，参见《项目管理系统填报指南》。

第二十一条 省级以上等保办在审核确认测评项目登记信息时，发现测评机构具有下列情形之一的，应不予审核通过。

（一）处于暂停测评业务期间；

（二）因违规被通报后，未反馈整改情况的；

（三）其他不符合本办法规定情形的。

第二十二条 属于异地测评项目的，测评机构应从项目管理系统中生成测评项目基本情况表，并于测评项目实施前报送或传至被测评网络备案公安机关。

第二十三条 测评机构名称、地址、测评人员、主要负责人和联系人发生变更的，测评机构应在变更后5个工作日内向等保办报告，并提交变更材料。

测评机构法人、股权结构发生变更或其他重大事项发生变更的，等保办应组织重新进行推荐审查并出具审查意见。测评机构不得假借变更名义转让推荐证书。

第二十四条 测评机构应加强对测评人员的监督管理，定期组织开展安全保密教育和测评业务培训，签订安全保密责任书，规定其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。

第二十五条 测评机构应组织测评师参加多种形式的测评业务和技术培训，测评师每年培训时长累计不少于40学时。培训时长不足的，不予年度注册。

测评联盟确定测评业务和技术培训科目，发布年度测评培训纲要。

第二十六条 测评师离职前，测评机构应与其签订离职保密承诺书，收回上岗证并及时向等保办报备。

自离职之日起超过6个月再入职测评机构的测评师，应通过测评师考试后从事测评活动；自离职之日起一年内未入职测评机构从事测评活动的，测评联盟应注销其测评师证书。

第二十七条 测评机构应监督测评师妥善保管测评师证书、上岗证，不得涂改、出借、出租和转让。

第二十八条 测评机构应当建立网络安全应急处置机制和纠纷处理机制，防范测评风险，妥善处理纠纷。

第二十九条 测评项目完成后，测评机构应请被测评单位对测评服务情况进行评价，评价情况表由被测单位密封后反馈测评机构，留存备查。

第三十条 测评机构应每季度向等保办报送测评业务开展情况和测评数据。根据测评实践，测评机构每年底编制并向等保办报送网络安全状况分析报告。

测评机构在测评活动中，发现重大网络安全事件、重大网络安全风险隐患、高危漏洞和重大网络安全威胁时，应及时报告公安机关。

第三十一条 国家等保办每年第四季度组织开展测评机

构能力验证活动，并将能力验证结果通报各省级等保办。

未参加能力验证的测评机构，视为能力验证未通过。

第三十二条 等保办应于每年12月份对所推荐测评机构进行年审。

年审通过的，等保办在推荐证书副本上加盖等级保护专用章或等保办印章，发放测评师注册标识。

年审时，测评机构应当提交以下材料：

（一）网络安全等级保护测评机构年审表；

（二）网络安全等级保护测评机构推荐证书副本；

（三）年度测评工作总结；

（四）测评师年度注册表；

（五）其他所需材料。

第三十三条 测评机构有下列情形之一的，年审不予通过。

（一）未及时、准确地填报测评项目信息；

（二）测评师培训时长不足；

（三）未定期报送测评业务开展情况和测评数据；

（四）能力验证未通过且整改方案落实不到位；

（五）其他有关情形。

年审未通过的，等保办责令测评机构限期整改。拒不整改或整改不符合要求的，应暂停测评机构开展等级测评业务。

第三十四条 测评机构推荐证书有效期为三年。测评机构应在推荐证书期满前30日内，向等保办申请期满复审。

等保办应于收到期满复审申请后5个工作日内，组织开展复审工作。复审通过的测评机构，由等保办换发新证。省级等保办应及时将测评机构期满复审情况报国家等保办汇总。

期满复审时，测评机构应提交以下材料：

（一）测评机构期满复审申请表；

（二）年审情况；

（三）其他需要提供的有关材料。

第三十五条 测评机构有下列情形之一的，期满复审不予通过。

（一）累计两年年审未通过或三年能力验证未通过的；

（二）基本条件不符合的；

（三）违反本办法有关规定且情形特别严重的；

（四）逾期30日未提交期满复审申请的。

期满复审未通过的，等保办应公告宣布取消其推荐证书。

第四章　监督管理

第三十六条 省级以上等保办对测评机构和测评业务开

展情况进行监督、检查、指导。

国家等保办每年组织对测评机构及测评活动开展监督抽查。

测评项目实施过程中，测评机构应接受被测网络备案公安机关的监督、检查和指导。

第三十七条 等保办开展监督检查时，重点检查以下内容：

（一）测评机构基本条件符合情况；

（二）测评机构管理制度执行情况；

（三）测评机构相关事项变更报告、审查情况；

（四）测评师管理、行为规范情况；

（五）测评项目实施情况；

（六）测评服务评价情况；

（七）测评报告及相关数据文档管理情况；

（八）其他需监督检查的事项。

第三十八条 等保办、被测网络备案公安机关在监督检查时，发现异地测评机构有违反本办法规定情形的，应书面通报该机构推荐等保办。

等保办在收到通报后，应及时组织进行核查处置并反馈，同时将有关情况报国家等保办。

第三十九条 等保办应及时将测评数据、测评机构及其测评师情况、年审和期满复审情况、监督检查情况等相关数

据录入数据库。

第四十条 国家等保办每年对全国测评机构开展年度评定活动，评定结果及时发布。

第四十一条 任何组织和个人有权向省级以上等保办、测评联盟投诉举报测评机构和测评人员违法违规行为。

第四十二条 测评机构违反本办法第十五、十六、十七、十八、十九、二十二、二十三、二十四、二十五、二十六、二十七、二十八、二十九、三十条规定，等保办应责令其限期整改；拒不整改或情形严重的，约谈测评机构法人和主要负责人；屡次违反上述规定或情形特别严重的，责令其暂停测评业务，并予通报。

第四十三条 测评机构有下列情形之一的，等保办责令其限期整改；情形严重的，责令整改期间暂停测评业务，并予通报。

（一）未按照有关标准规范开展测评，或未按规定出具测评报告的；

（二）分包、转包、代理测评项目，或恶意竞争，扰乱测评工作正常开展的；

（三）擅自简化测评工作环节，或未按测评流程要求开展测评工作的；

（四）监督检查或抽查中发现问题突出的；

（五）影响被测评网络正常运行，或因测评不到位，未

发现网络中存在相关漏洞隐患，导致被测评网络发生重大网络安全事件的；

（六）非授权占有、使用，以及未妥善保管等级测评相关资料及数据文件的；

（七）限定被测评单位购买、使用指定网络安全产品，或与产品和服务商存在利益勾结行为的；

（八）非本机构测评师或测评人员未取得等级测评师证书和上岗证从事等级测评活动的；

（九）未通过测评项目管理系统及时填报项目登记信息或未通过审核开展等级测评项目的；

（十）未按本办法规定向等保办提交材料或弄虚作假的；

（十一）其他违反本办法有关规定行为的。

第四十四条 测评机构有下列情形之一的，等保办应取消其推荐证书，并向社会公告，三年内不得再次申请。

（一）运营管理不规范，屡次被责令整改，严重影响测评服务质量的；

（二）因单位股权、人员等情况发生变动，不符合测评机构基本条件的；

（三）有网络安全产品开发、销售或系统安全集成等影响测评结果公正性行为；与产品提供商、服务商或被测评方存在利益勾结，扰乱测评业务正常开展的；

（四）泄露被测评单位工作秘密、重要数据信息的；

（五）隐瞒测评过程中发现的重大安全问题，或者在测评过程中弄虚作假未如实出具等级测评报告的；

（六）一年内未开展测评业务（被暂停开展测评业务的情况除外）或自愿放弃测评机构推荐资格的；

（七）连续两年年审未通过或未通过期满复审的；

（八）测评实施期间，导致被测评网络发生宕机等严重网络安全事件的；

（九）有第四十二条、第四十三条情形，造成特别严重后果或影响特别恶劣的；

（十）其他违反法律法规或严重违反本办法规定情形的。

第四十五条 测评师有下列行为之一的，等保办责令测评机构督促其限期改正；情节严重的，责令测评机构暂停其参与测评业务；情形特别严重的，应注销其测评师证书，责令其所在测评机构进行限期整改。

（一）未经允许擅自使用、泄露或出售等级测评活动中收集的数据信息、资料或测评报告的；

（二）违反本办法规定，有涂改、出借、出租和转让测评师证书、上岗证等行为的；

（三）测评行为失误或不当，严重影响网络安全或造成被测评单位利益重大损失的；

（四）其他违反本办法有关规定行为的。

第四十六条 测评机构及其测评师违反本办法的相关规定，给网络运营者造成严重危害和损失，构成违法犯罪的，由相关部门依照有关法律、法规予以处理。

第四十七条 公安机关有关工作人员在工作中不得利用职权索取、收受贿赂；不得滥用职权、干预测评机构及测评业务正常开展，以及法律法规禁止的其他行为。

第四十八条 本办法自发布之日起实施。本办法由国家等保办负责解释。

第四十九条 自本办法实施之日起，《信息安全等级保护测评机构管理办法》、《信息安全等级保护测评机构异地备案实施细则》、各地自行制定的与本办法规定不符的规范性文件一律作废。

第五十条 本办法所称“以上”含本数。