淮南市数据资源管理局
中共淮南市委网络安全和信息化委员会办公室
淮南市公安局
淮南市财政局 文件

淮数资〔2025〕10号

关于进一步做好全市网络安全等级保护测评工作的通知

市直各单位:

为进一步提高全市信息安全防护水平,统筹做好全市网络安全等级保护测评工作,发挥统一招标采购优势,提高财政资金使用绩效,现将有关事项通知如下:

一、根据淮南市网络安全等级保护测评服务框架协议采购结果，确定安徽省电子产品监督检验所等6家单位为淮南市2025-2027年度网络安全等保测评服务供应商,服务期限为2025年7月至2027年6月。

二、有网络安全等保测评服务需要的单位可在入围的6

家供应商中任意选取1家或多家作为服务供应商，直接签订合同，不需另外招标。

三、网络安全等保测评服务价格按照二级等保1.72万元、三级等保3.1万元的定价执行，禁止超范围、超标准采购等保测评服务，所需资金由各部门在预算中统筹。

四、各单位要切实履行主体责任，严格落实网络安全等保要求，对本单位信息系统应测尽测，在订立等保测评采购合同后及时向市数据资源局备案，测评结束后按合同约定组织验收，对中标供应商开展服务质量和测评质量评估。网络安全等级保护测评报告按要求提交到属地公安机关网安部门审核，并在公安部登记管理系统完成填报。市委网信办、市公安局、市财政局、市数据资源局将不定期对各单位等保落实情况进行监督检查。

五、各县区、各相关企业可参照此通知执行。

附件：1. 网络安全等保测评服务框架协议入围供应商名单

2. 等保测评服务框架协议主要内容

淮南市数据资源管理局

中共淮南市委网络安全和信息化委员会办公室

淮南市公安局

淮南市财政局

2025年7月30日

附件 1：

网络安全等保测评服务框架协议
入围供应商名单

序号	机构名称	联系方式
1	安徽省电子产品监督检验所	15056247990
2	中检集团天帷网络安全技术（合肥）有限公司	15955147041
3	杭州安信检测技术有限公司	18156066590
4	安徽国康网络安全测评有限公司	18712075501
5	北方实验室（沈阳）股份有限公司	13721066997
6	安徽溯源电子科技有限公司	17855122766

附件 2：

等保测评服务框架协议主要内容

一、项目概况

1.1 项目背景

随着数字技术的迅猛发展，数字技术已融入政府机关工作和人民生活的方方面面，网络安全的重要性日益凸显。根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》的规定，网络安全等级保护制度已经成为我国网络安全领域的基本制度。公安部、保密局、国密局、国信办联合印发《信息系统安全等级保护管理办法》（公通字〔2007〕43 号）等相关文件，要求在全国范围的政府机关、企事业单位开展信息安全等级保护建设工作。根据《关键信息基础设施安全保护条例》规定，电子政务领域信息系统在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

淮南市级预算单位建设、使用的信息系统众多、结构复杂、分布区域广泛，信息系统所承载的业务和数据涉及公民、法人或其他组织的合法权益、公共利益，以及社会秩序和国家安全等，安全性要求高。

为全面贯彻落实网络安全等级保护制度，统筹做好市级

预算单位网络安全等级保护测评工作，发挥集中采购优势，提升财政资金使用绩效，市数据资源管理局组织开展了市级预算单位等级保护测评对象情况摸底工作，经过摸底梳理及确认，现需要淮南市购买等保测评服务框架协议采购项目，对淮南市级预算单位网络安全等级保护测评对象（以下简称“等保对象”）进行等级保护测评，提升市级预算单位网络安全整体水平。

1.2 项目目标

深入贯彻《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等法律法规，全面落实《党委（党组）网络安全工作责任制实施办法》，按照国家有关网络安全等级保护标准要求，完成市级预算单位网络安全等级保护测评（以下简称“ 等保测评”）服务工作，确保国家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落到实处。完成淮南市级预算单位等保测评工作，包括测评准备、定级与备案支撑、测评实施、安全培训和安全风险排查等内容。

1.3 测评范围

本次测评范围涉及互联网、市政务外网等保对象所属单位业务专网，部署环境涉及云平台、虚拟化、传统服务器等多种架构，设备类型涉及 PC 服务器、小型机、各类专用网络和安全设备等。

1.4 测评依据

服务提供方应依据但不限于以下标准中相应级别安全要

求，开展安全评估和等级测评。如发布最新标准，应按照国家有关要求，依据最新标准开展评估测评工作。

1.《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）；

2.《国家信息化领导小组关于加强信息安全保障工作的意见》（中办〔2003〕27 号文件）；

3.《信息安全等级保护管理办法》(公通字〔2007〕43 号)；

4.关于印发《信息系统安全等级测评报告模版（试行）》的通知（公信安〔2015〕2866 号）

5.《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）；

6.《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）；

7.《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）；

8.《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）；GB/T 25058-2019《信息安全技术网络安全等级保护实施指南》；

9.《信息安全技术网络安全等级保护测试评估技术指南》（GB/T 36627-2018）；

10.《关键信息基础设施安全保护条例》；

11.《中华人民共和国网络安全法》；

12.《中华人民共和国数据安全法》；

13.《关于推动信息安全等级保护测评体系建设和开展等

级测评工作的通知》（公信安〔2010〕303号）；

14.《省级预算单位网络安全等级保护测评服务集中统一采购工作实施方案（试行）》（皖数资〔2022〕6号）。

二、供应商类型

等保测评服务企业

三、第一阶段入围供应商的评审方法

质量优先法

四、第二阶段成交供应商的方式确定

直接选定

五、合同服务地点及期限

在签订等保服务合同时根据市直有关单位实际需求确定服务地点，等保测评服务期限为1年。

六、框架协议期限

自框架协议签订之日起2年。

七、服务需求

7.1需求总概

本项目是对淮南市级预算单位开展等保测评工作，项目主要内容包括：测评准备、定级与备案支撑、测评实施、安全培训和安全风险排查四大项。

7.2测评准备

包括前期调研、数据分析、测评方案编制等。具体包括编制和配合填报信息系统基本情况调查表，开展面对面访谈进一步了解等保对象情况；准备评估工具，汇总和分析调研数据，完成测评工作方案编制。

7.3 定级与备案支撑

对未定级备案的各等保对象的定级、备案以及材料准备等工作提供咨询和指导服务，协助等保对象所属单位完成系统定级备案工作。

1.协助定级。协助等保对象所属单位对等保对象情况进行分析，通过分析等保对象所属类型、所属信息类别、服务范围，了解系统的可用性、完整性、保密性需求，清晰确定保护对象，确定受侵害的客体、客体受侵害的程度，最终确定等保对象的系统服务保护等级和业务信息保护等级，协助等保对象所属单位编制定级报告等。

2.协助备案。协助等保对象所属单位填写《信息系统安全等级保护备案表》，并到公安部门完成系统备案工作，协助等保对象所属单位取得《备案证明》。

7.4 测评实施

包括现场测评、提出安全整改建议、配合安全整改、出具测评报告。具体内容如下:

1、现场测评。服务提供方需到现场开展测评工作，对信息系统的物理环境、网络和通信、计算环境、应用和数据、管理制度、管理机构和人员、建设运维等方面进行全面评估分析，开展漏洞扫描和渗透测试，查找与等级保护基本要求之间的差距。

（1）安全技术测评为以下五个方面：安全物理环境：机房位置、访问控制措施、防盗窃和破坏措施、防雷击措施、防火措施、防水防潮措施、防静电措施、温湿度控制措施、

电力供应措施、电磁防护措施；安全通信网络：网络架构、通信传输、可信验证；安全区域边界：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件、安全审计、可信验证；安全计算环境：网络设备、安全设备、服务器、终端、系统管理平台、数据库、业务应用软件、业务数据和个人信息；安全管理中心：系统管理、审计管理、安全管理、集中管控；

（2）安全管理测评为以下五个方面：安全管理制度：安全策略、管理制度、制定和发布、评审和修订；安全管理机构：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查；安全人员管理：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理；安全建设管理：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择；安全运维管理：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、 密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理。

（3）工具测试：对等保对象开展漏洞扫描、渗透测试和巡检安全服务工作。

（4）基础工具（包括但不限于）： 漏洞扫描、渗透测试工具

2、提出安全整改建议。服务提供方现场测评后要对等保对象的安全现状和风险进行分析，形成相应的安全问题列表和整改建议，并协助制订和完善符合相应等级的等保对象安

全整改技术方案。

3、配合安全整改。若经过现场测评存在安全风险，服务提供方需配合等保对象所属单位进行安全整改。针对等保对象，提供与等级保护标准存在差异的相关网络安全配置加固、高危风险修复、安全策略制定等技术整改指导服务；提供针对网络安全制度的整改，包括但不局限于：各项信息安全管理制度的制定、修订、落实，及相关记录完善等，规范信息安全日常管理工作，提高信息安全基础管理水平。

4、出具测评报告。上述所有工作完成后，供应商在 15 天内出具符合等保行业标准的网络安全等级保护测评报告，一份提交至等保对象所属单位，一份提交到属地公安机关网安部门审核，并在公安部登记管理系统完成填报。

7.5 安全培训和安全风险排查

1、安全培训

（1）服务提供方须为等保对象所属单位提供不少于 1 次的网络与信息安全培训服务，培训内容包括国家等级保护制度、系统定级原则方法、等级保护测评工作流程、信息安全策略、信息保密制度、信息安全管理制度等。

（2）服务提供方须提供培训计划，包括培训内容、课时安排等。

2、安全风险排查

在等保服务有效期内，二级等保对象每半年提供 1 次漏洞扫描，每年度提供 1 次渗透测试服务；三级等保对象每季度提供 1 次漏洞扫描，每半年提供 1 次渗透测试服务，重要

时期的漏洞测试和渗透测试服务不局限于上述服务时间次数，按照相关主管部门和服务对象单位要求开。

八、服务要求

8.1 技术服务总则

1、工作优先原则。服务提供方提供的服务以顺利推进项目工作优先为原则;

2、人员稳定原则。服务提供方需为此项目配备专门的管理人员和技术人员，并提供了统一、专有和固定的服务管理接口，包括专有的项目负责人接口和服务工程师接口，保持人员稳定，确保沟通顺畅;

3、及时汇报原则。服务提供方应定期向项目组织方和等保对象所属单位汇报项目和服务工作情况、存在问题，紧急问题应当天当时及时汇报;

4、安全保密原则。服务提供方应严格遵循安全保密原则，对服务过程中涉及的任何用户及等保对象信息，未经允许不得向其他任何第三方泄露，以及不得利用这些信息损害采购人及等保对象所属单位利益;

5、记录规范原则。服务人员应做好工作记录，以便采购人和等保对象所属单位跟踪监督、统计考核，确保能提供完整的服务清单。

8.2 对入围供应商及选派人员的服务要求

1、入围供应商须提供不少于 4 名专业技术人员到现场开展等保测评服务，进场时查验人员资质证书；非经等保对象所属单位许可，入围供应商不得中途更换选派人员。

2、入围供应商选派人员要服从等保对象所属单位的工作安排，认真履行职责，保质保量完成约定的各项工作任务。入围供应商在签订服务合同后，无故拖延超过 10 个工作日不进场工作的，等保对象所属单位有权终止合同。

3、严格遵守相关工作纪律，保守工作中涉及的国家秘密及商业秘密个人隐私。

8.3 验收要求

1、质量标准供应商提供的服务质量标准应按照中华人民共和国相关标准及相应的技术规范、采购文件中相关要求、等保测评相关服务标准及相应的技术规范中要求执行。

2、验收组织等保对象所属单位负责组织验收工作。

3、验收程序

（1）供应商在完成相关服务后，向等保对象所属单位提交验收材料，申请验收。

（2）等保对象所属单位成立验收小组，验收人员应由等保对象所属单位代表和技术专家组成。

（3）验收通过后由验收方出具验收报告，首次验收发生的检测（检验）费、劳务报酬等费用支出，由等保对象所属单位承担。因供应商问题验收不合格导致重新组织项目验收的，如采购合同有约定按照约定执行，如无约定，由等保对象所属单位承担。

8.4 保密要求

服务提供方必须与等保对象所属单位签订保密协议，对项目实施过程中接触的设备信息、数据资料等负有保密责任，

不得泄露给任何第三方。

8.5 供应商退出机制

1 年服务期内，服务的等保测评对象发生网络安全事件，或在各级组织的攻防演练被攻破，或经主管部门监测发现系统安全问题，且相关问题或漏洞在等保测评中未发现、测评报告中未体现（0day 漏洞除外），累计达到 3 次以上；征集人收到等保测评对象所属单位书面投诉累计 3 次以上；所属测评报告与往期报告高度雷同，存在抄袭情况；以低于第二阶段定价与业主方另签协议的。征集人将出现以上情况的供应商进行退出处理，且下一年度原则上不再征集该供应商。