安徽医科大学信息系统等级保护测评服务采购项目政府采购合同

（服务类）

项目名称：安徽医科大学信息系统等级保护测评服务采购项目

项目编号：25AT186017103635/FS34000120253616 号

追 踪 号：202504130002

甲方（采购人）：安徽医科大学

乙方（成交供应商）：中移系统集成有限公司

签订地： 安徽医科大学

签订日期：2025 年 7 月 7 日

安徽医科大学（以下简称：甲方）通过安徽安天利信工程管理股份有限公司组织的竞争性磋商方式采购活动，经磋商小组评定，中移系统集成有限公司（以下简称：乙方）为本项目成交供应商，现按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》、《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经甲方和乙方协商一致，约定以下合同条款，以兹共同遵守、全面履行。

1.1 合同组成部分

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 成交通知书；

1.1.3 响应文件（含澄清或者说明文件）；

1.1.4 磋商文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

1.2 服务

1.2.1 服务名称：安徽医科大学信息系统等级保护测评服务采购项目；

1.2.2 服务内容：信息系统等保测评（二级）、信息系统安全托管服务，详见招标文件内容；

1.2.3 服务质量：合格，符合甲方要求。

1.3 价款、履约保证金

1.3.1本合同总价为：￥658000.00元（大写：人民币陆拾伍万捌仟元整）

1.3.2履约保证金为：￥16450.00元（大写：人民币壹万陆仟肆佰伍拾元整），退还时间：验收合格且无违约情形下退还。

分项价格：

序号	分项名称	分项价格
1	信息系统等保测评（二级）	470400元
2	信息系统安全托管服务	187600元
总价		658000元

1.4 付款方式和发票开具方式

1.4.1 付款方式：“信息等级保护测评（二级）”服务结束后，第一次验收，验收通

过后支付对应款项。“信息系统安全托管服务”结束后，第二次验收，验收通过后支付合同余款；

1.4.2 发票开具方式：开具增值税普通发票。

甲方开票信息：

单位名称：安徽医科大学

开户银行：建设银行合肥市贵池路支行

账　　号：34001454508050007226

1.5 服务期限、地点和方式

1.5.1 服务期限：自合同签订之日起一年；

1.5.2 服务地点：合肥市安徽医科大学，采购人指定地点；

1.5.3 服务方式：符合招标文件规定和甲方要求。

1.6 违约责任

1.6.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式履行，那么甲方可要求乙方支付违约金，违约金按每迟延履行一日的应提供而未提供服务价格的0.25 %计算，最高限额为本合同总价的 2.5 %；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

1.6.2 除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 0.25 %计算，最高限额为本合同总价的 2.5 %；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

1.6.3 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或者隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同；

1.6.4 任何一方按照前述约定要求违约方支付违约金的同时，仍有权要求违约方继续履行合同、采取补救措施，并有权按照己方实际损失情况要求违约方赔偿损失；任何一方按照前述约定要求解除本合同的同时，仍有权要求违约方支付违约金和按照己方实际损失情况要求违约方赔偿损失；且守约方行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.6.5 除前述约定外，除不可抗力外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.6.6 如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响成交结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

1.6.7 因甲方未按合同约定支付价款、未按合同约定受领标的物、擅自解除合同、逾期退还履约保证金导致乙方遭受的直接损失，乙方可向甲方申请赔偿，赔偿金额由双方协商一致；针对因政策变化等原因不能签订合同或解除合同时，造成乙方合法利益受损的情形，可以给予乙方合理补偿，补偿金额不得超过乙方的直接损失。

1.7 服务需求

1.7.1 建设背景

依据《中华人民共和国网络安全法》《信息安全等级保护管理办法》及《安徽省高等学校教育信息化建设评价指标体系2.0（试行）》，落实信息系统等级保护措施，进一步提高安徽医科大学信息系统的整体安全防护能力。本次项目计划采购一套信息系统等级保护测评服务，测评学校部分重要信息系统，并引入网络安全防护第三方服务，提升学校网络安全保障能力。

1.7.2 建设目标

通过信息系统等级保护二级测评，实现信息系统等级保护二级框架下的物理环境、网络架构、边界防护、安全审计、可信验证、供应链、移动安全、数据备份和恢复、安全制度等维度的安全测评和强化。

引入网络安全防护第三方服务提升安徽医科大学校内部重要资产的漏洞闭环处置率；缩短安全威胁的发现时间和响应时间；减少校内产生危害的安全事件数量；重要资产配备云端专业安全团队进行7*24小时的值守，提高安全运营成熟度。

1.7.3 建设内容

1.7.3.1 信息系统等级保护测评服务

拟对安徽医科大学重要信息系统实施等级保护测评，以进一步完善信息系统安全管理体系和技术防护体系，切实提高系统信息安全防护能力，为信息化建设的健康有序发展提供可靠保障。

本次信息系统网络安全等级保护测评需就信息系统进行等级保护测评。乙方应依据相应等级的安全保护测评要求及行业的特殊安全需求，对信息系统网络安全进行等级保护符

合性测评。测评内容涵盖物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、数据安全与备份恢复、安全策略和管理制度、安全管理机构和人员、系统建设管理、系统运维管理等信息安全的各个层面。

要求测评机构以国家等级保护相关标准《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》为基础，对学校整体信息系统的构成、应用情况、网络结构、安全现状加以分析研究、编制信息系统测评技术方案和实施方案，可以按照国家政策最新标准及要求进行，提交差距分析、问题清单及整改意见、测评报告、等一系列技术文档。

1.7.3.1.1 12个核心业务信息系统进行测评（须取得相关等保测评证书）

完成对12个学校核心业务系统信息系统等级保护测评（二级）。

待测评系统分为12个类，具体清单为：安防管理、财务管理、采购管理、对外交流、科研和实验管理、人事和政务管理、图书档案管理、团学管理、网站群、学科和教学管理、智慧校园、资产管理。

1.7.3.1.2 等级保护测评主要包括以下几个方面

（1）等保测评：完成包括安全物理环境、安全计算环境、安全区域边界、安全通信网络、安全管理中心和安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理方面的测评工作。

（2）工具测试：**针对本次测评的信息系统进行漏洞扫描、渗透测试等安全服务工作。**

乙方需基于CVE、CNVD、CNNVD等漏洞数据库，通过扫描等手段对指定的远程或者本地的网络设备、主机、数据库、操作系统、中间件、业务系统等进行安全弱点检测，最终输出《漏洞扫描报告》。

乙方需利用主流的攻击技术和工具对目标网络、业务系统、数据库进行模拟黑客攻击测试，将发现的安全漏洞进行整理，给出详细说明，并针对每一个安全漏洞提供相应的解决建议，最终输出《渗透测试报告》和《渗透测试复测报告》。

（3）整改建议：乙方应根据现场测评中发现的问题，分析与GB/T 22239-2019、ISO/IEC 27001、ISO/IEC 20000、ISO 22301、ITIL和ITSS等行业最佳实践之间的差距，按照网络安全等级保护标准要求提出安全整改建议。

（4）编制测评报告：完成上述测评工作和整改加固实施后，乙方最后出具符合标准要求的信息系统网络安全等级保护测评报告。

1.7.3.1.3 实施原则

（1）规范性原则：乙方工作中的过程和文档，具有很好的规范性，可以便于项目的

跟踪和控制。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

（3）可控性原则：测评的工具、方法和过程需在双方认可的范围之内并符合进度表的安排，保证学院对服务工作的可控性。

（4）整体性原则：测评和分析的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

（5）最小影响原则：测评工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响(包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在应答书上详细描述)。

（6）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害学院网络的行为，否则学院有权追究责任。

1.7.3.1.4 测评依据

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

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

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

《信息安全技术 网络安全等级保护测评过程指南》（GB／T 28449-2018）。

1.7.3.1.5 等级保护测评内容

根据国家等级保护相关标准，本次项目的网络安全等级保护测评应包括以下内容：

（1）安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评。

①安全物理环境

安全物理环境是对机房和办公场所的物理环境安全防护情况进行测评，包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等方面的安全状况。

②安全通信网络

安全通信网络测评是对网络系统安全防护情况进行测评，包括网络架构、通信传输、可信验证等方面的安全状况。

③安全区域边界

安全区域边界是对边界防护、访问控制、入侵防范、恶意代码防范、安全审计、可信验证等方面的测评。

④安全计算环境

安全计算环境是对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面的测评。

⑤安全管理中心

安全管理中心是对系统管理、审计管理、安全管理、集中管控等方面的测评。

（2）安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评。

①安全管理制度

安全管理制度测评是对安全策略、管理制度、制定和发布、评审和修订进行测评。

②安全管理机构

安全管理机构测评是对岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等情况进行测评。

③安全管理人员

安全管理人员测评是对人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等情况进行测评。

④安全建设管理

安全建设管理测评是对建设过程中安全方案设计、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、服务供应商选择等情况进行测评。

⑤安全运维管理

安全运维管理测评是对环境管理、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、外包运维管理等情况进行测评。

1.7.3.1.6 网络安全等级保护合规治理服务

对信息资产进行全量细颗粒度梳理、脆弱性标记、威胁标记，对资产建立逻辑关系并可视化展现等。服务对象不仅包含传统资产关联平台的硬件、软件，并且对人员、管理制度等多种类型信息资产分类管理。

1.7.3.1.7 主要项目内容包括

（1）漏洞扫描：供应商需针对网络设备，服务器，应用等进行漏洞扫描，出具漏洞扫描报告。

（2）渗透测试：模拟黑客可能使用的攻击技术和漏洞发现技术，对信息系统进行验

证性渗透测试。

（3）安全加固：发现合规差距并协助进行安全加固，包括修复系统漏洞、优化网络边界防护策略（如防火墙规则、入侵检测）、强化身份认证与访问控制（RBAC、多因素认证）、完善日志审计与数据加密（存储/传输）、制定应急预案及管理制度。

（3）系统定级与备案：协助学院完成系统的定级（含专家评审）与备案工作，最终取得公安部门下发的备案证明。

（4）等级保护测评：完成安全技术层面包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全测评；安全管理层面包括安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。完成上述测评工作和整改加固实施后，最后出具符合公安机关要求的各信息系统网络安全等级保护测评报告。

（5）所有工作完成后需提供以下材料：

①问题清单及整改建议；

②信息系统网络安全等级保护测评报告；

③配合校方取得等保测评备案证书。

1.7.3.2 信息系统安全托管服务

本次项目要求提供10个核心业务系统的安全托管服务和10个系统的渗透测试，服务期为一年。重要保障时期和攻防演练期间，提供现场安全运维服务。安全托管服务期间，安全专家团队需要对学校的托管资产进行7*24小时的安全值守，并且在节假日期间值守；对发现的安全问题，需要结合学校现状给出处置建议并协助学校闭环安全事件。安全托管服务具体要求如下：

★（1）乙方需为学校提供服务成果展示门户，应具备服务质量可视化展示，能通过可视化的数据，清晰的了解安全专家的服务水平。至少包括脆弱性闭环率、脆弱性平均响应时长、脆弱性平均闭环时长、威胁闭环率、威胁平均响应时长、威胁平均闭环时长、事件闭环率、事件平均闭环时长。

★（2）应当提供云端检测和分析平台，为学校提供7*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示，平台支持将同一资产的多个告警进行聚合分析发现各类安全事件并生成工单，并在告警详情中展示告警的基本信息。

（3）针对服务范围内资产扫描到的高危可利用漏洞，乙方应当为学校做好每一个高危可利用漏洞的防护工作，包括但不限于为学院提供漏洞修复方案和安全设备防护策略，以及帮助学院配置防护规则，保证学院不因此出现重大事件和损失。

（4）乙方提供的安全专家每月对学校的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果；乙方云端服务平台应当具备丰富的策略检查工具。

（5）为了保障服务质量和加强乙方与学校的沟通，乙方应当承诺为学校线上配置一名经验丰富的安全专家作为专属服务经理，并且实时响应学校咨询的网络安全相关问题。

（6）为了保证安全监测的准确率和服务质量，服务应当支持为学校自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求。

★（7）服务中的云端服务平台应当支持对接学校网络中已部署的态势感知平台和防火墙，支持实时接收态势感知平台和防火墙检测到的安全事件信息、安全日志数据。

（8）服务中的云端服务平台支持对接收到的安全设备数据进行分析，可跳转到学校现有安全态势感知平台上进行安全事件处置。

（9）乙方提供的服务成果展示门户可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《准备阶段文件》、《特殊时期值守报告》、《运营周报》、《运营月报》、《运营季报》、《威胁情报》、《年度汇报》、《事件总结报告》。

（10）乙方应承诺对重大事故启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，2小时上门处置；对服务范围内发现的每一个高危可利用漏洞提供有效防护规则。

1.7.4 项目实施

1.7.4.1 人员团队：乙方拟派的安全服务团队不得少于4人。

（1）项目经理1名，需满足安全等级测评师资质。

（2）安全托管服务经理：不少于1名，具备10年以上相关工作经验，熟练掌握网络安全技术，包括但不限于防火墙配置、安全策略制定、漏洞扫描工具使用等。

（3）线下安全服务工程师：不少于2名，具备3年以上渗透测试、漏洞扫描经验，能够熟练运用各种渗透测试工具和方法，对目标系统进行全面、深入的漏洞挖掘，准确评估系统安全风险。

现场测评结束后，提供一年的售后服务，售后服务期内根据业主需求能及时安排参与现场测评的测评师到达现场协助和指导整改工作。

1.7.4.2 计划实施进度：乙方需在中标后7个工作日内与乙方对接，详细了解学校的网络架构、业务系统、安全需求等相关信息，并收集必要的技术资料，包括但不限于网络拓扑图、业务系统清单等。

1.7.4.3 实施过程管理：

（1）数据备份与安全措施

乙方在实施渗透测试和漏洞扫描前，需对学校的关键业务系统和数据进行备份操作，确保在测试过程中不会对现有数据造成损坏或丢失。

数据备份完成后，乙方需进行数据恢复测试，验证备份数据的完整性和可用性，并将测试结果形成报告提交给学校备案。

乙方需在实施过程中采取必要的安全措施，确保测试活动不会对学校的网络、系统和数据安全造成威胁。乙方应提前对测试活动进行全面的风险评估，识别可能存在的风险点，并制定相应的风险应对措施。

风险评估报告需提交给学校审核，学校有权要求乙方对高风险环节进行优化调整，乙方需在5个工作日内完成调整并重新提交审核。

（2）测试实施与监控

乙方需按照项目实施规划，严格遵守学校的网络和系统访问权限要求，开展渗透测试和漏洞扫描工作。测试过程中，乙方应详细记录测试步骤、发现的漏洞、漏洞利用方法、测试结果等内容，并形成完整的测试记录。

在实施过程中，乙方需确保测试活动的合法性和合规性，不得对学校的业务系统进行未经授权的攻击或破坏行为。如因乙方的不当操作导致学校业务系统出现故障或数据丢失，乙方需承担相应的法律责任和经济赔偿。

（3）漏洞修复与验证

乙方在完成渗透测试和漏洞扫描后，需向学校提供详细的漏洞修复建议书，建议书应包括漏洞描述、风险等级、修复方法、修复步骤等内容，并协助学校进行漏洞修复工作。

乙方需在学校进行漏洞修复过程中提供技术支持，及时解答学校在修复过程中遇到的问题，并根据学校的需求，提供必要的现场技术支持服务。

学校完成漏洞修复后，乙方需在15个工作日内对修复结果进行验证，确保漏洞已彻底修复且未对系统功能造成影响。验证完成后，乙方需出具漏洞修复验证报告，报告应详细记录验证方法、验证结果等内容，并提交给学校备案。

1.7.5 数据标准或系统集成

无

1.7.6 保密要求

乙方需在项目实施过程中对相关文档进行严格管理，包括项目实施规划、测试记录、漏洞报告、修复建议书、项目进展报告、项目总结报告等。

所有文档需按照学校的要求进行编号、归档，并确保文档的完整性和准确性。项目结

束后，乙方需将所有文档的电子版和纸质版提交给学校存档。

1.7.7 项目培训

针对等级保护测评安全管理工作，为学校提供注册信息安全专业人员或数据安全相关培训不低于2次。

1.8 合同争议的解决

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择下列第 1.8.2 种方式解决：

1.8.1 将争议提交 / 仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.8.2 向 项目所在地 人民法院起诉。

1.9 合同生效

本合同一式陆份，每份具有同等法律效力，本合同自双方法定代表人或授权代表签字并盖章和见证方盖章后生效。

甲　　方：　安徽医科大学

（单位盖章）

法定代表人

或授权代表

（签字）：

时间：　2025 年 7 月 7 日

乙　方：　中移系统集成有限公司

（单位盖章）

法定代表人

或授权代表

（签字）：

时间：　2025 年 7 月 6 日

乙方账户信息

户名：中移系统集成有限公司

账号：8888 0151 0000 2818

开户银行：招商银行股份有限公司北京分行营业部

见证方：（单位盖章）

日期：2025 年 7 月 9 日