合同编号：HNTQ2024-CP071

郑州大学信息化办公室、网络管理中心采购网络安全综合治理管控服务及等保网络安全防护项目（包2）

合同

甲方：郑州大学

乙方：河南天祺信息安全技术有限公司

依照《中华人民共和国民法典》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，甲乙双方就本服务采购相关事项协商一致，共同达成如下协议：

一、合同内容及要求：

详见附件1（附后）。

二、合同总价款：

本合同价格为人民币（大写）贰拾捌万玖仟元整（小写：￥289000.00元）（含税）。该合同价格包括乙方提供实施服务发生的差旅费、食宿费及履行本合同下其他所有义务所需的费用。

三、质量要求或服务标准，乙方对质量负责的条件和期限：

质量要求（服务标准）：通过公安网安部门备案，获得其颁发的备案证明（以当年网安政策部门为准，二级复测系统市局不换发新证），提交甲方验收，以验收报告为准。

质保期为：自验收合格之日起一年。

四、服务约定：

1、服务完成时间：自合同签订起30个日历天内。

2、服务地点：郑州大学。

3、服务方式：现场测评。

五、验收标准、方法：（需提供三份验收资料）

测评结束后，乙方提交以下文档，并经甲方确认无误后，视为验收通过。

1、 网络安全等级保护测评报告

2、 网络安全等级保护整改建设方案

3、 网安部门颁发的《信息系统安全等级保护备案证明》（以当年网安政策部门为准，二级复测系统市局不换发新证）

六、结算方式及期限：合同初验付 70%，终验合同尾款 30%。

七、免费质保约定：

免费提供一年的质保期，质保期内免费提供信息安全咨询工作，免费提供信息安全应急及时响应工作。

八、售后服务承诺

1、 提供 7*24 小时热线服务，对用户提出的信息安全等级保护问题给予及时、专业的解答，必要时可达现场提供紧急情况的应急支持服务，确保在 4 小时内解决问题。

2、 定期的回访咨询以及工程师现场巡检等服务，保证服务质量，以及保障信息系统的安全防护能力。

3、 技术问题解答、咨询和规划等，通过电话、即时通讯、EMAIL 等方式与用户进行在线服务。

4、 长期为客户提供免费的技术咨询服务，帮助客户规划后续的安全解决方案。

5、 等级保护相关知识培训。

九、履约担保

合同总价款 10 万元（含 10 万元）至 100 万元（不含 100 万元）不强制提供保函或现金履约担保，由甲方和乙方双方协商。

十、违约责任：

1、乙方违约：乙方提供的服务内容不符合约定的质量要求或服务标准，甲方有权解除或终止合同，并要求乙方按合同总价款的 5%支付违约金，给甲方造成经济损失的，乙方还应按给甲方造成的经济损失赔偿；乙方未按约定期限交付标的物，每迟延一天须按合同总价款的 1%向甲方支付违约金。如果乙方对合同迟延履行超过合理期限，甲方有权解除或终止合同，并且要求乙方赔偿由此给甲方造成的经济损失。

2、甲方违约：甲方未能按双方约定的方式和期限支付合同价款，按有关法律规定对乙方承担违约责任。

3、双方其他违约责任按《中华人民共和国民法典》的有关规定处理。

十一、争议解决

双方在执行合同时产生纠纷，协商解决；协商不成，向甲方所在地人民法院提起诉讼。

法律文书寄送地址（乙方）：郑州市高新区碧桃路 20 号郑州高新企业加速器产业园 D 区 D5-2 栋

十二、其它约定事项：无

十三、本合同未尽事宜经双方协商可另订补充协议。

十四、本合同正本 贰 份、副本 捌 份，发包人执 肆 份，承包人执 肆 份，报送招标代理机构 贰 份。

十五、本合同自甲乙双方签字并盖章之日起生效，随合同履行完成而自行终止。

甲方（盖章）：郑州大学

法定代表人或代理人：

单位地址：郑州市科学大道 100 号

电话：0371-67781903

开户银行：工商银行郑州中苑名都支行

户名：郑州大学

帐号：1702021109014403854

签定日期：2024. 9. 14.

签约地点：郑州

乙方（盖章）：河南天祺信息安全技术有限公司

法定代表或代理人：

单位地址：郑州市高新区碧桃路 20 号郑州高新企业加速器产业园 D 区 D5-2 栋

电话：0371-67579921

开户银行：中国工商银行股份有限公司郑州中苑名都支行

户名：河南天祺信息安全技术有限公司

帐号：1702021109200049642

签定日期：2024年9月14日

附件 1：服务需求及要求

包 2：技术要求：

1. 等保测评服务

（1）按照网络安全等级保护定级标准和工作要求，**协助我校完成在公安部门的等级保护全面测评工作，测评内容包括：定级、现场测评与备案**工作。

（2）按照国家等级保护相关标准和要求，对我校信息系统开展网络安全等级保护测评工作，查找安全差距，**提交安全整改建议和等级测评报告；**

（3）本项目按照网络安全等级保护 2.0 技术标准进行网络安全等级测评。

（4）对我校相关网络安全人员的专业技能培训以及安全运维等其它服务工作。

（5）供应商应配备相应技术人员满足本项目服务需求。

（6）一个三级等保测评系统，四个二级等保测评系统。

（7）校内 30 个系统的内部测评和管理员测评培训。

2.1 测评系统范围

依据《教育行业信息系统安全等级保护定级工作指南》，本次等保测评系统包含：一个三级系统，四个二级系统。针对上述信息系统，按照《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）、《计算机信息系统安全等级保护划分准则》、《教育行业信息系统安全等级保护定级工作指南（试行）》等文件要求，对本项目涉及的以上重要信息系统开展信息系统安全等级保护测评工作，发现可能存在的问题，提交安全整改建议，并出具公安部门认定的系统安全保护等级测评报告；遵循适度安全原则，综合考量成本与效益因素，制定信息系统安全等级保护整改方案，指导整改工作。协助学校完成整改，以达到等级保护相关文件的要求，完成信息系统安全保护等级备案工作，并按招标人要求在公安部门取得备案证明。

具体包括但不限于以下工作：

（1）记录各系统运行现状及安全状况

记录被测信息系统的基本情况（可参考信息系统安全等级保护备案表），包括但不限于：系统的运营使用单位、投入运行时间、承载的业务情况、系统服务情况以及定级情况。

（2）等级测评结果

对等级测评结果进行汇总统计，通过对信息系统基本安全保护状态的分析给出等级测评结论。

（3）制定《网络安全等级保护测评报告》

列出被测信息系统中存在的主要问题以及可能造成的后果，制订《网络安全等级保护测评报告》。

（4）制定《网络安全等级保护整改建设方案》

在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订《网络安全等级保护整改建设方案》。

（5）协助指导等级保护测评整改工作

针对系统存在的主要问题提出安全建设、整改建议，协助完成系统整改工作。

2.2 测评内容

测评内容主要包括两个方面：一是单元测评，测评指标与《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）相应等级的基本要求完全一致；二是系统整体测评，主要测评分析信息系统的整体安全性。

单元测评包括安全技术测评和安全管理测评两大部分，其中安全技术测评层面主要包含：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。安全管理测评层面主要包含：安全管理制度、安全管理人员、安全管理机构、安全建设管理、安全运维管理。

整体测评在单元测评的基础上进行进一步测评分析，在内容上主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等。

（1）安全物理环境

主要包含物理位置选择、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、电磁防护等方面的内容。

（2）安全通信网络

主要包含网络架构、通信传输、可信验证等方面的内容。

（3）安全区域边界

主要包含边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的内容。

（4）安全计算环境

主要包含身份鉴别、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内容。

（5）安全管理中心

主要包含系统管理、审计管理、安全管理、集中管控等方面的内容。

（6）安全管理制度

主要包含安全策略、管理制度、制定和发布、评审和修订等方面的内容。

（7）安全管理机构

主要包含岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面的内容。

（8）安全管理人员

主要包含人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等方面的内容。

（9）安全建设管理

主要包含定级和备案、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、服务供应商选择等方面的内容。

（10）安全运维管理

主要包含环境管理、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、外包运维管理等方面的内容。

2. 测评要求

3.1 需遵循的政策法规及行业规范

要求与《信息安全等级保护管理办法》（公通字[2007]43号）、《信息系统安全等级保护实施指南》（信安字[2007]10号）和《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号）等公安部网络安全等级保护系列文件要求保持一致。

■ 《中华人民共和国数据安全法》（2021年9月1日）

- 《中华人民共和国网络安全法》（2017 年 6 月 1 日）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）
- 《信息安全技术 网络安全等级保护设计技术要求》（GB/T25070-2019）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）
- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）
- 《信息系统通用安全技术要求》（GB/T20271-2006）
- 《信息系统等级保护安全设计技术要求》（GB/T25070-2010）
- 《计算机信息系统安全等级保护通用技术要求》（GA/T390-2002）
- 《计算机信息系统安全等级保护管理要求》（GA/T391-2002）
- 《信息安全技术 信息系统安全等级保护实施指南》（GB/T25058-2010）
- 《信息安全技术 网络安全等级保护定级指南》（GBT 22240-2020）
- 《网络安全等级保护测评报告模板》（公安部最新模板）
- 《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]429 号）
- 《信息安全等级保护管理办法》（公通字[2007]43 号）
- 《信息安全技术 网络基础安全基础要求》 （GB/T20270-2006）
- 《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 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）
- 《信息安全风险评估规范》GB/T 20984-2007
- 《信息技术安全性评估准则》GB/T 18336-2001
- 《关于加强教育行业网络与信息安全工作的指导意见》
- 《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》
- 《河南省教育厅 河南省公安厅关于深入开展教育行业信息系统安全等级保护工作的通知》（教科技【2015】710 号文件）

3.2 保密要求

（1） 投标方承担委托方的保密责任，在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。

（2） 未经双方书面同意，不得向第三方透露项目和涉及双方单位信息安全、 技术成果的任何内容。

（3） 项目结束后，双方必须互相确认信息安全服务过程中提供的相关资料，相互承担保密责任。

3.3 测评过程交付成果

交付项目各阶段测评过程文档（参照《信息安全技术 网络安全等级保护测评过程指南》），见下表（包括但不限于）。

项目阶段	交付成果
测评准备活动	信息调研表
方案编制活动	信息系统安全测评方案
现场测评活动	测评结果记录 测评中发现的问题汇总
分析与报告编制活动	信息系统安全等级测评报告

3.4 整改建议要求

（1）整改建议

依照《信息安全等级保护安全建设整改工作指导意见》（公信安[2009]1429号），严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，在系统测评工作的基础上，对信息系统总体信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全建设整改方案，方案内容包含：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全建设整改技术方案设计、安全建设整改管理体系设计、信息系统安全产品选型及技术指标建议、安全建设整改项目实施计划、项目预算，整改后可能存在的其他问题。

（2）技术要求

涉及所有被测评系统的安全整改方案，需包含如下内容：

方案分项	详细内容及要求
等级化安全保障建议方案	内容应包括但不限于以下方面： 1. 安全区域和等级划分； 2. 安全体系框架设计； 3. 等级化安全指标体系报告。

安全体系建设建议方案	内容应包括但不限于以下方面： 1. 网络面临风险分析； 2. 针对性措施建议。
相关网络安全 管理制度	内容应包括但不限于以下方面： 1. 机房安全管理制度； 2. 网络故障应急预案及应急方案流程制度； 3. 客户端管理制度； 4. 数据备份及恢复制度； 5. 灾难恢复策略及制度。

（3）项目交付成果及要求

提供不同测评阶段对应的各项文档，及最终的安全等级测评报告，以及切实可行的安全防护整改建议书等。包括但不限于：

1）《网络安全等级保护测评报告》

2）《网络安全等级保护整改建设方案》

3）网安部门颁发的《信息系统安全等级保护备案证明》

交付要求：交付项目涉及的所有业务系统的安全等级测评整改技术方案对应的文档，及其对应的网络安全等级保护测评报告原件。

3. 服务期要求

等保测试为合同签订后 30 个日历天 ；

4. 售后服务

（1） 提供 7*24 小时热线服务，对用户提出的信息安全等级保护问题给予及时、专业的解答，必要时可达现场提供紧急情况的应急支持服务，确保在 4 小时内解决问题。

（2） 定期的回访咨询以及工程师现场巡检等服务，保证服务质量，以及保障信息系统的安全防护能力。

（3） 技术问题解答、咨询和规划等，通过电话、即时通讯、EMAIL 等方式与用户进行在线服务。

（4） 长期为客户提供免费的技术咨询服务，帮助客户规划后续的安全解

决方案。

（5） 等级保护相关知识培训。