一、项目背景

《中华人民共和国网络安全法》是国家安全法律制度体系中的一部重要法律，是网络安全领域“依法治国”的重要体现，2017 年 6 月 1 号起正式施行。《网络安全法》第二十一条、第三十一条明确规定“国家实行网络安全等级保护制度”、“落实国家等级保护制度，突出保护重点”。网络安全等级保护制度是国家网络安全保障工作的基本制度、基本策略和基本方法，完善国家网络安全保障体系，强化关键信息基础设施、重要信息系统和数据资源保护，提高网络综合治理能力，是促进信息化健康发展，维护国家安全、社会秩序和公共利益的根本保障。

为深入贯彻党中央有关文件精神和《网络安全法》，有效应对当前网络安全面临的严峻威胁与挑战，全力做好学校重要信息系统网络安全保卫工作，现对其开展等保评测工作，及时发现系统安全隐患并迅速进行整改，从而全面提升重要信息系统的网络安全防护水平，有效防范网络安全威胁，保障系统的安全、高效、稳定运行。

二、项目范围

序号	等保测评系统名称	定级
1	站群系统	二级
2	学工系统	二级
3	教务系统	二级

三、项目测评内容

（一）项目依据

按照网络安全等级保护 2.0 标准开展本次等保测评工作，测评的指标、内容及其程序需严格执行如下规范要求：

《中华人民共和国网络安全法》

《信息安全等级保护管理办法》(公通字[2007]43 号)

《信息系统安全保护等级定级指南》（GB/T 22240-2008）

《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 网络安全等级保护安全设计技术要求》(GB/T 25070-2019)

《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）

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

《信息系统安全管理测评》（GA/T 713-2007）

《信息安全等级保护等级测评实施细则》

《信息安全风险评估规范》（GB/T 20984-2007）

《信息安全风险管理指南》（GB/Z 24364-2009）

《信息安全管理体系要求》（GB/T 22080-2008）

《信息安全管理实用规则》（GB/T 22081-2008）

《信息系统安全管理要求》（GB/T 20269-2006）

《信息安全事件分类分级指南》（GB/Z 20986-2007）

《信息安全事件管理指南》（GB/Z 20985-2007）

《信息系统灾难恢复规范》（GB/T 20988-2007）

《信息安全应急响应计划规范》（GB/T 24363-2009）

（二）服务内容及说明

1.等保保护测评

等保测评覆盖安全技术测评和安全管理测评两大类10个方面。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、安全计算环境和安全管理中心等5个层面上的安全控制测评；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5个方面的安全控制测评。

1.1等保测评内容

根据国家对网络安全等级保护工作的相关法律和技术标准要求,结合本项目的系统保护等级开展实施与之相应的检查工作，具体检查内容应包括：

（1）安全物理环境

测评内容主要包括：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、电磁防护等。

（2）安全通信网络

测评内容主要包括：网络架构、通信传输、可信验证等。

（3）安全区域边界

测评内容主要包括：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。

（4）安全计算环境

测评内容主要包括：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。

（5）安全管理中心

测评内容主要包括：系统管理、审计管理、安全管理、集中管控等。

（6）安全管理制度

测评内容主要包括：安全策略、管理制度、制定和发布、评审和修订等。

（7）安全管理机构

测评内容主要包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等。

（8）安全管理人员

测评内容主要包括：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。

（9）安全建设管理

测评内容主要包括：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。

（10）安全运维管理

测评内容主要包括：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。

1.2 等保测评目标

（1）识别信息安全风险。通过对信息系统在安全技术和安全管理方面的分析，发现信息系统在安全技术和安全管理方面与相应安全等级保护要求之间的差距，并进行风险分析，出具差距分析报告，明确信息系统面临的风险。

（2）增强安全防护能力。依据差距分析报告的结果，并结合实际情况，区分轻重缓急，制定针对性的安全整改计划，通过安全整改不断提高信息系统的整体安全保护水平。

（3）测评结果分析

单项测评结果判定

单元测评结果判定

整体测评分析

形成测评分析报告

针对测评分析报告的整改建议

2.渗透测试

选取可能发起攻击的测试点，使用渗透测试的方式查找可能存在的渗透点，发现信息系统防护体系的薄弱环节，找出可能发生的恶意攻击事件和违规行为。

2.1 渗透测试内容

工作内容包括渗透测试及提供漏洞修复方案。本次渗透测试工作为黑盒测试。

（1）需要包含如下阶段

前期交互阶段：与用户组织进行讨论，确定渗透测试范围和目标。

信息搜集阶段：采用各种方法搜集用户方的所有相关信息。

威胁建模阶段：使用在信息搜集阶段所获取到的信息，标识出目标系统上可能存在的安全漏洞与弱点。

漏洞分析阶段：综合前面几个环节获取到的信息，从中分析和理解，找出攻击途径和攻击方法。

渗透攻击阶段：针对确定好的攻击途径和攻击方法实施渗透攻击，获取系统相关权限。

后渗透攻击阶段：以特定的业务系统作为目标，识别出关键的基础设施，找出用户组织最具价值和尝试进行安全保护的信息和资产，找出能够对用户组织造成重要业务影响的攻击途径。

报告阶段：将渗透测试结果编制成文档提交给用户，提供安全解决方案。并将在渗透测试阶段产生的垃圾数据进行清理。

（2）渗透测试工作要求

本次渗透攻击测试工作应当以不破坏用户应用系统为前提条件，不做危害用户应用系统的工作行为，遵守职业道德，遵守行业规则，严格遵守保密制度，保密要求，不得擅自修改、拷贝用户数据，不得泄露、传播用户的敏感信息，如有违反将负法律责任。

（三）服务成果

本次安全服务应提交以下成果：

《信息系统等级测评报告》，包括单元测评分析结果、整改测评分析结果、测评结论和安全整改建议等。

四、项目总体要求

1、合同签订后60个工作日内完成相关测评工作。测评单位需根据学校实际情况合理安排测评进度，学校可能因为各类突发状况导致测评周期的不确定性，供应商需要配合学校进行进度的合理安排。项目工作人员需遵守等保检测规定，采用符合标准的检测工具和检测方法实施检测，如因违规操作造成对检测系统的破坏，则应承担相应责任。

2、测评单位必须针对此次测评给出详细方案，内容包含测评计划、测评实施、风险管控、协助整改。要求方案充分考虑到高校特性，结合业务要求，提出切实可行的整改方案。

3、测评单位需针对此次测评列出本项目组织管理架构及主要参与人员情况介绍。要求组织管理架构及人员配备科学完整，项目负责人、项目组人员有参与高校项目的管理经验。项目实施过程中实行专人专职原则，保证各安全层面的测评全面有效，能够发现实际存在安全风险，现场实施人员均需持有等级保护测评师证书。项目组人员必须熟练掌握信息安全相关标准与规范，具备丰富的信息安全测评工作经验，具有成熟的信息安全技术和项目管理能力，能够应对可能的突发性安全事件应急工作。

4、供应商必须单独配备安全测评工具，包含但不限于以下种类工具：网络漏洞扫描系统、web 漏洞扫描系统。供应商必须在技术方案内明确专项检查所需要的所有技术检测工具，至少包含以下内容：名称、型号、主要功能、数量等。

5、在测评过程中保证客观性和公正性原则，测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案开展。

6、测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。详细描述在测评过程中如何通过技术手段控制和规避可能对学校业务系统造成的影响。对于项目实施过程中出现的异常情况如何处理，保证学校系统正常运行以及测评的可进行性。

7、协助整改，针对差距测评结果，给学校提出合理、可行的整改方案和建议，并在整改完毕后给出系统定级报告。

8、提供详尽、明确的技术培训，同时提供本次乃至后续的培训方案，方案应包含网络安全相关课程内容以及详细培训体系流程。

★9、本次等级保护测评项目不得转包或者分包，所有驻场测评师必须持证上岗，未经采购方同意，项目组成员不得更改，**响应文件中须提供至少两名现场测评师人员信息及现场测评师所持有的《网络安全等级测评师证书》复印件，并提供谈判供应商为现场测评师缴纳的2023年8月至10月中任意一个月的社保证明，未提供或不符合要求则视为无效响应。**

★五、项目实施方案要求

供应商需根据本项目服务内容编制详细的项目实施方案，

项目实施方案内容可参考：

1、测评内容、测评指标；

2、测评工作流程；

3、测评工作的详细实施方案；

4、测评过程中的渗透测试服务方案；

5、测评工具的详细介绍；

6、培训方案；

7、人员配置方案；

8、供应商认为需要提供的其它方案，

供应商可按以上目录编制本项目实施方案，但以上目录并无限制性，供应商可根据自身情况调整及编制本项目实施方案。

未提供项目实施方案则视为无效响应。

六、报价要求：

供应商应当在合同签订后60个工作日内完成采购文件规定的项目并交付学校使用。

七、项目验收标准及要求：

项目完成后，供应商须按照项目采购服务内容及要求，按国家、行业或企业等标准，提供相应的服务内容及交付成果，供应商完成全部项目内容并经采购人验收合格后，项目整体验收合格。

八、承包方式：固定总价包干

九、付款方式：

成交供应商完成项目合同的所有工作，经采购人确认无误后，于15个工作日内支付项目额的100%款项。付款前成交供应商应向采购人开具发票，采购人收到发票并确认无误后向成交供应商支付相应款项。

十、项目预算价：

本项目预算金额：人民币15万元。

本项目最高限价：人民币15万元，供应商投标报价不得高于最高限价，否则作为无效响应处理。