网络安全等级保护测评服务采购清单

一、项目需求

《中华人民共和国网络安全法》自 2017 年 6 月 1 日起施行，“要求网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。

网络安全等级保护工作以保护信息系统为核心，严格参考等级保护关于相关管理规范和技术标准，从多个层面进行评估，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、安全管理中心和安全管理等层面，判定受测系统的技术和管理级别与所定安全等级要求的符合程度，基于符合程度给出是否满足所定安全等级的结论，针对安全不符合项提出安全整改建议，为信息系统稳定运行提供有力保障。

1、测评系统级别

序号	系统名称	等保测评级别
1	教务管理系统	二级
2	招生管理系统	二级

2、标段

本次招标为两个二级系统，投标文件一式三份，正本一份，副本两份。

3、测评时间要求

本次测评项目签订合同后 2 个月内完成，具体项目流程分为前期准备、现场实施、报告分析与编制、检查验收、总结验收五个阶段。

4、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，结合系统保护等级开展实施与之相应的测评工作，完成网络安全等级保护的测评后，提交信息系统的测评报告至本地公安等保办，等保测评主要包括以下内容：

1)安全物理环境

安全物理环境具体包括 10 个控制点：

物理位置的选择、 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。

2)安全通信网络

安全通信网络具体包括 3 个控制点：

网络结构、通信传输、可信验证。

3)安全区域边界

安全区域边界具体包括 6 个控制点：

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。

4)安全计算环境

安全计算环境具体包括 11 个控制点：

身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信计算、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。

5)安全管理中心

安全管理中心具体包括 4 个控制点：

系统管理、审计管理、安全管理、集中管控。

6)安全管理制度

安全管理制度具体包括 3 个控制点：

管理制度、制定和发布、评审和修订。

7)安全管理机构

安全管理机构具体包括 5 个控制点：

岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

8)安全管理人员

安全管理人员具体包括 4 个控制点：

人员录用、人员离岗、安全意识教育及培训、外部人员访问管理。

9)安全建设管理

安全建设管理具体包括 10 个控制点：

系统定级、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。

10) 安全运维管理

安全运维管理具体包括 14 个控制点：

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。

5、测评实施原则

1） 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，按照评估双方相互认可的评估方案，基于明确定义的测评方式和解释，实施评估活动。

2） 可重复性和可再现性原则

依照同样的要求，使用同样的评估方式，对每个评估实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同评估者评估结果的一致性有关，后者与同一评估者评估结果的一致性有关。

3） 连续性原则

确保在高速变化的信息安全环境中，在有效的服务期间内，保证采购方风险评估结论的准确性和及时性，对于采购方单位新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。从经济上，降低了采购方单位的成本，从信息安全性上，保证信息安全测评的动态稳定性。

4） 扩展性原则

在评估过程结束后，信息安全测评过程要保持扩展性，从扩展的属性上进一步加强测评结束后采购方的安全管理有效性和可用性。

5） 保密原则

在测评过程中，需严格遵循保密原则，双方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购方利益。

6） 互动原则

在整个测评过程中，强调采购方的互动参与，每个阶段都能够及时根据采购方的要求和实际情况对测评的内容、方式做出相关调整，进而更好的进行风险评估工作。

7） 最小影响原则

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。

8） 规范性原则

网络安全等级保护测评服务的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

9） 质量保障原则

在整个测评过程中，须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督，控制项目的进度和质量。

10）系统安全原则

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。

11）测评人员原则

为了保证本次测评项目的实施质量和工期，本项目采用项目经理负责制，供应商安排具备一定安全技术能力、项目管理工作经验与等级保护测评工作经验丰富的人员担任项目经理。测评实施方工作人员必须通过公安部的等级保护等级测评师认证，持证上岗，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，须经采购方确认资格后方可实施测评工作。

12）项目进场实施前，供应商必须与采购人签订项目保密协议。

二、评分标准

（一）价格分：10 分

以进入评标程序、满足采购文件要求且报价最低的投标报价为评标基准价（须未超过采购预算或最高限价（如有），其价格分为满分 10 分。其他投标人的价格分统一按照下列公式计算：

投标报价得分=（评标基准价/投标报价）╳价格权值╳100（价格权值为 10%）

（二）测评方案：55 分

1、测评项目理解比较（10 分）

根据对信息系统理解选择相应的标准，必须真实、合理、可执行，内容完整全面，能真实反应信息系统当前的安全状况，并能根据测评结果给出相应的整改建议得 10 分，内容比较全面，能基本反应当前安全状况得 7 分，项目理解不全面，有缺项、漏项得 4 分。其余情况不得分。

2、测评服务方案的完整性和专业性比较（25 分）

（1）测评方案中需包含测评工作流程详细规范，测评内容、测评指标、测评方法具有合理性与可操作性得 10 分，测评内容、指标较明确但可操作性一般得 7 分，测评内容、指标、方法不太明确，并不具备可操作性得 4 分。（10 分）

（2）等级保护测评过程中的风险规避措施，措施有效合理得 10 分，措施比较有效合理得 7 分，规避措施无针对性得 4 分。（10 分）

（3）提供明确系统渗透测试方法，渗透测试方案清晰得 5 分，渗透测试方案不合理且得 2 分。（5 分）

3、施工组织、培训方案比较（20 分）

（1）实施方案有制定详细的进度安排和人员保障计划，能把握时间节点按进度提供项目文档，人员和计划安排得当、时间进度合理得 7 分，人员和计划安排基本合理、时间进度一般 4 分，人员和计划安排较差不够合理得 1 分。（7 分）

（2）针对此次测评提供明确的培训方案，方案具有针对性、可操作性，内容涵盖网络安全相关的内容；方案具有针对性、内容较全面得 7 分，方案针对性一般，内容较全面得 4 分，方案针对性较差，内涵涵盖不全面得 1 分。（7 分）

（3）重要信息系统安全事件到场响应服务时间为 1 小时内（含 1 小时）得 6 分；响应服务时间为 2 小时内（含 2 小时）得 3 分；响应服务时间为 3-12 小时内（含 12 小时）得 1 分；响应服务时间超过 12 小时不得分。投标单位注册地在苏州或外地机构在苏州有分公司的，在苏州交社保人员不少于 15 人，需提供社保证明。（6 分）

（三）测评质量保证：14 分

1、针对本项目配备的项目经理具有高级测评师、CISP 证书有一个得 2 分，最高得 4 分，须提供响应单位为上述人员连续缴纳近 2 个月的社保证明及相应证书复印件并加盖响应单位公章。 （4 分）

2、测评组其他测评师比较：10 分

具有高级测评师证书、PMP 证书、ITIL 证书、CISP-DSG 证书、国家网络安全应用检测专业测评人员证书，有一个得 2 分，最高 10 分；须提供响应单位为上述人员连续缴纳近 2 个月的社保证明及相应证书复印件并加盖响应单位公章。（本项最高 10 分）

（四）磋商响应企业综合能力比较：12 分

1、市级以上（含市级）网络安全技术支撑单位，得 2 分；

2、信息安全风险检查评估机构备案证明，得 2 分。

3、投标人具有软件能力成熟度 CMMI3 证书，得 2 分；

4、投标人具有高新技术企业证书，得 2 分；

5、投标人具有工业信息安全检测评估机构证书，得 2 分；

6、投标人具有工业信息安全应急处置机构证书，得 2 分。

（五）磋商响应企业规范性比较：9 分

1、投标人具有质量管理体系认证证书的，得 3 分；

2、投标人具有信息安全管理体系认证证书（认证内容含等级保护测评与风险评估服务相关）的，得 3 分；

3、投标人具有信息技术服务管理体系认证证书，得 3 分。

苏州工业园区职业技术学院招标委员会

2021 年 11 月 24 日