单位名称（公章）：

联系人及联系方式：

**一、项目名称：**2024年网络安全等级保护测评项目

**二、预算金额：**25万元，服务期为一年。

**三、项目概况：**

为贯彻落实国家网络安全等级保护制度，进一步加强安徽建筑大学信息系统的整体安全防护能力，明确安徽建筑大学各信息系统的安全防护水平与国家网络安全等级保护相关要求之间的差距以及存在的安全隐患，现需对安徽建筑大学的5个信息系统进行网络安全等级保护测评服务（1个3级，4个2级），出具公安部门认可的网络安全等级保护测评报告并提供相应安全服务（渗透测试、漏洞扫描、重保服务等）。

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）

**四、付款方式**

服务期满后一次性付款。

**五、服务范围及要求**

**（一）服务范围**

项目内容为对安徽建筑大学的5个信息系统进行网络安全等级保护测评服务，出具公安部门认可的网络安全等级保护测评报告，并提供相应安全服务；被测评系统名称如下：

|  |  |  |
| --- | --- | --- |
| **序号** | **待测系统名称** | **安全保护等级** |
| 1 | 科研管理信息系统（省级） | 3 |
| 2 | 安徽建筑大学办公自动化系统（新OA） | 2 |
| 3 | 研究生管理信息系统 | 2 |
| 4 | 综合人事管理系统 | 2 |
| 5 | 财务系统 | 2 |

1. **服务总体要求**

1、等保测评工作具体内容包括如下：

（1）测评范围

安全技术测评：对采购人被测系统涉及的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等技术层面进行现场测评和差距分析，记录相关的测评结果。

安全管理测评：对采购人安全管理机构、安全管理制度、安全人员管理、安全建设管理、安全运维管理等管理层面进行现场测评和差距分析，记录相关的测评结果。

（2）形成差距分析报告

依据测评结果和测评标准，对安徽建筑大学被测评系统进行安全现状分析，形成相应的差距分析报告，为下阶段开展整改工作提供依据。

（3）编制整改建议书

依据测评标准，结合差距分析报告，编制针对安徽建筑大学被测评系统的整改建议书。

（4）形成等级测评结论及测评报告提交

完成上述等保测评工作和整改后，由中标人出具符合标准要求的《等级保护测评报告》。

1. 安全服务工作具体内容包括如下：

（1）漏洞检测服务（2次）

提供全网服务器主机漏洞扫描，利用漏洞扫描工具主动发现系统、主机存在的脆弱性，能对服务范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络设备、服务器主机、数据和用户账号/口令等扫描对象中存在的安全风险、漏洞等。漏扫服务发现的漏洞需站在业务视角进行梳理分析，提供专业有效的解决方案，并配合进行漏洞整改方案的实施。

漏洞扫描类型需包含：

1. 操作系统
2. 数据库
3. 常见应用服务
4. Web应用程序
5. 网络设备及安全设备
6. Web 服务器
7. 电子邮件系统

每次漏扫服务实施完成后5个工作日内，中标人需向采购人提供：《XXX 漏扫测试服务报告》。

漏洞检测服务主要是使用专业的漏洞评估产品及人工验证方式，检测操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议,共2次

（2）渗透测试服务（2次）

由安全工程师模拟黑客的行为模式，采用黑客的漏洞发现和利用技术，以及尽可能多的攻击方法，对目标应用系统的安全性进行深入分析。渗透测试对象包括互联网应用服务系统（WEB系统）以及相关的其他系统。对WEB系统的渗透测试，需要在互联网网络的任一位置进行渗透测试；对内部系统的渗透测试，必须在内部办公网络进行渗透测试并提供渗透测试报告。

漏洞类型包含不限于：

1. 跨站脚本
2. SQL注入
3. 代码执行
4. 目录遍历
5. 文件包含
6. 脚本源码泄露
7. 物理路径泄漏
8. 应用错误信息
9. 备份文件

渗透手段包含不限于：

1. 对 WINDOWS、LINUX 等操作系统本身进行渗透测；
2. 对 ORACLE、MYSQL 等数据库应用系统进行渗透测试；
3. WEB 应用系统渗透；
4. 网络设备渗透，对各种防火墙、入侵检测系统、网络设备进行渗透测试；
5. 对系统业务进行渗透，对系统的核心业务进行安全风险挖掘；
6. 口令猜解；
7. 其它渗透，除了上述的测试手段以外的技术测试手段。

每次渗透测试服务实施完成后5工作日内，中标人需向采购人提供《XXX系统渗透测试报告》。

（3）网络安全培训服务（2次）

投标人需要为采购人提供线上或线下的信息安全技术培训， 由具备专业培训资格的讲师参考国家重要信息系统安全保障人员（CIIPT）、注册信息安全专业人员（CISP）、网络安全能力认证培训人员（CCSC）、信息安全保障人员（CISAW）等安全技能培训认证课程内容授课，确保管理人员和技术人员掌握关于信息系统等级保护相关规范、信息安全策略、信息保密制度，信息安全管理制度和相关流程等。（一次意识培训，一次技术培训）

（4）应急演练（1次）

依据法律法规、国际国内标准、行业监管要求等，在总体预案框架下，从业务层面、技术层面，并充分考虑各类灾难场景，帮助客户制定各类应急预案，提升各类突然事件的应急响应速度，保证业务及信息系统正常运行。网络安全应急演练保障活动共分为启动阶段、准备阶段、演练阶段、保障阶段、总结阶段五个阶段，具体工作安排计划如下：

启动阶段：确定演练目标、人员团队职责划分、演练总体流程，后续工作提供指导。

准备阶段：需对演练目标进行安全分析和梳理，开展全面安全评估、关注现有安全能力、完成安全策略的全面优化、人员的全面赋能等。

演练阶段：重点检测演练系统的监测手段和防御手段的有效性及安全人员操作规程熟悉度。

保障阶段：为保障业务系统的平稳运行，避免因安全问题而导致出现重大事故。

总结阶段：对行动中发现的相关问题进行快速整改并进行总结，将经验固化至相关的规章制度中，形成常态化、制度化。

每次应急演练服务实施完成后5工作日内，中标人需向采购人提供《应急演练报告》。

（5）重要安全保障服务

根据要求提供重要时期安全保障服务的服务支持，包括互联网侧风险排查、内部网络风险排查、现场值守服务；

重保期间实时关注安全设备和态势感知平台的攻击事件，对于未拦截高、中危的攻击事件，及时更新或优化安全策略；不能确认的攻击行为，及时联系安全厂商进行研判。对于安全设备访问和流量日志，如果出现频繁访问某一源IP地址，向客户确认后，进行手工阻断处理。

重要安全保障服务工作量：一人值守，不少于2次，总共不少于7天。

每次重要安全保障服务完成后5个工作日内，中标人需向采购人提供：《XXXXX 重要时期安全保障日报》、《XXXXX 重要时期安全保障工作总结》。

**（三）考核要求**

中标人按招标文件要求，完成等保评测规定的工作内容，提供相关过程文档，能够出具符合要求的结果报告。

|  |  |
| --- | --- |
| **时间段** | **提交文档** |
| 签订合同后 | 《测评服务技术方案》  《测评服务工作计划表》 |
| 差距测评阶段 | 《等级保护差距分析报告》  《整改建议书》  符合等级保护要求的各项安全管理制度 |
| 等保测评验收 | 符合公安机关要求的《等级保护测评报告》 |

1. **商务部分调研【各单位请根据本单位实际情况填写】**

|  |  |  |
| --- | --- | --- |
| **评分内容** | **评分标准** |  |
| 项目人员 | 投标人针对本项目需求拟配备的项目团队应设置质量经理、项目经理等，具体评审指标如下：   1. 质量经理：   是否具有高级等级测评师证书；  是否具有注册信息安全专业人员（CISP）证书；   1. 项目经理：   是否具有高级测评师证书；  是否具有信息安全保障人员认证（CISAW）证书或具有注册信息安全专业人员（CISP）证书；   1. 团队成员（最少2人）：   是否全部具有初级（含）以上等级测评师证书；  是否具有一个及以上高级等级测评师证书；  具有中国信息安全测评中心颁发的注册信息安全专业人员（CISP）证书或信息安全保障人员认证（CISAW）证书；  **注：提供以上证书等证明材料原件的清晰扫描件，不提供不得分。** | □是 / □否  □是 / □否  □是 / □否  □是 / □否  □是 / □否  □是 / □否  个 |
| 投标人业绩 | 投标人是否具有10个及以上自2021年01月01日以来的等保测评服务业绩合同（以合同签订日期为准）  **说明：投标文件中须提供业绩合同的扫描件/复印件,合同扫描件至少提供封面、服务内容和签字盖章页。** | □是 / □否 |
| 投标人实力 | 是否具有质量管理体系认证证书；  是否具有信息安全管理体系认证证书；  是否具有信息技术服务管理体系认证证书；  是否具有检验检测机构资质认定证书（CMA）证书且检验检测的能力范围包括网络安全等级保护测评；  是否具有中国合格评定国家认可委员会（CNAS）颁发的检验机构认可证书且资质认定能力范围包含网络安全等级保护测评相关内容；  具有中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质证书的服务资质等级；  是否具有中国网络安全审查技术与认证中心颁发的信息系统安全运维服务资质认证证书；  具有网络安全等级保护方面的计算机软件著作权登记证书；  **注：1.以上证书须在投标文件中提供证书扫描件或复印件。 投标文件中须提供证书扫描件（复印件）或官方查询结果截图。** | □是 / □否  □是 / □否  □是 / □否  □是 / □否  □是 / □否  级服务资质  □是 / □否  个 |

**七、其他方面的建议**