

# 网络安全技术服务项目询价公告

各投标人：

舟山市教育服务中心对以下项目在政采云平台电子卖场进行在线询价采购，现邀请合格供应商参与响应报价。

## 一、采购项目内容

- 1、项目名称：网络安全技术服务
- 2、项目预算（最高限价）：9万元
- 3、采购类别：服务
- 4、采购内容：网络安全技术服务
- 5、采购数量：以采购内容要求为准
- 6、技术/服务要求：

注：标记为“▲”的重要参数，负偏离导至无效响应。

## 二、技术服务内容和要求

### 1、漏扫及渗透测试服务

指标项	指标要求
服务频率	漏洞扫描每年4次，渗透测试每年1次
服务范围	舟山市教育局政务云上系统（包括信息系统的移动app端）
服务内容	通过真实模拟黑客使用的工具、分析方法对信息系统进行模拟攻击，并结合智能工具扫描结果，由高级工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题。主要分析内容包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误等以及其他专项内容测试与分析，重点发现信息系统应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险，输出渗透测试报告。

交付物	《漏洞扫描报告》、《渗透测试报告》	
▲ 工具要求	系统及WEB应用扫描工具	<p>投标人在提供服务时，系统及WEB应用扫描工具应同时满足扫工具一和漏扫工具二，提供交叉扫描服务：</p> <p>漏扫工具一：</p> <ol style="list-style-type: none"> <li>1、支持检测的漏洞数大于20万条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供功能截图和CVE Compatible证书。</li> <li>2、产品支持对系统漏洞扫描、web漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表，请提供功能截图。</li> <li>3、提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。请提供功能截图。</li> <li>4、内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术，请提供功能截图。</li> <li>5、支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统，提供功能截图。</li> <li>6、支持扫描大数据组件框架的漏洞，需覆盖Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hdfs、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Yarn、Zookeeper，要求能够扫描大于300条相关漏洞，请提供功能截图。</li> <li>7、支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测；请提供功能截图。</li> <li>8、支持Oracle、MySQL、MS SQL、DB2、Sybase数据库漏洞检查，请提供功能截图。</li> <li>9、支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态，请提供功能截图。</li> </ol> <p>漏扫工具二：</p> <ol style="list-style-type: none"> <li>1、产品应具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》，请提供相关截图。</li> <li>2、产品应与统信服务器操作系统满足兼容认证要求，应通过统信UOS认证，请提供相关截图。</li> <li>3、产品应与银河麒麟高级服务器操作系统满足兼容认证要求，应通过麒麟软件NeoCertify认证，请提供相关截图。</li> <li>4、支持主机资产发现，采用TCP_SYN、ICMP_ECHO、UDP、TCP_ACK、SCTP等不低于5种发现方式，同时支持IPV6扫描，并支持探活端口设置，全天候巡检发现资产更新并展示，请提供功能截图。</li> <li>5、支持包括防火墙、交换机、路由器、服务器、摄像头、应用系统等31类资产识别，资产指纹总数不少于2万条，并支持自动对资产所属设备类型进行归类展示，请提供功能截图。</li> <li>6、支持企业信息识别，包括企业名称、官网、营业期限、电话、邮箱、子</li> </ol>

	<p>公司等，请提供功能截图。</p> <p>7、支持企业互联网服务主机信息发现，包括服务主机地址、端口、服务指纹、信息来源、发现时间等，请提供截图。</p> <p>8、支持 CMS 应用漏洞检测，通过 POC 原理扫描精准检测，CMS 插件数量不少于 2500 个，请提供功能截图。</p> <p>9、支持 Web 漏洞扫描，基于 URL 地址、周期、设置监控选项、并进行 cookies、重点页面、排除页面、爬虫深度、爬取 URL 数、爬虫并发数、扫描频率的设定进行扫描，支持 SQL 注入，XSS 跨站脚本，命令执行等 54 种常见通用漏洞类型扫描，不少于 3000 条通用漏洞规则，请提供功能截图。</p> <p>10、支持弱口令漏洞检测及数据泄漏监控，检测范围支持 MySQL,SSH,FTP,SQLServer,Redis 等服务数量不少于 24 种服务，支持 HTTP 网站表单弱口令扫描，支持弱口令字典自定义，请提供功能截图。</p> <p>11、支持登录扫描 linux 主机基线合规情况，检查项不少于 250 条，包括但不限于主机初始设置、服务配置、网络配置、日志审计、认证授权、系统维护等；检查结果包括风险等级、影响资产、检查项描述、检查操作、修复建议等；检查方式支持在线和离线，请提供功能截图。</p>
--	---

## 2、重保值守及应急响应服务

指标项	指标要求
期限频率	按需提供
服务范围	现场值守时间不少于 10 天
服务内容	<p>1、应急响应服务：信息系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏，造成系统不能正常运行时；已经发现的有可能造成上述现象的安全隐患，如非授权访问、信息泄密、系统性能严重下降、蠕虫或大面积爆发病毒等，当出现安全事件时，必须及时进行响应并提供《应急响应报告》。</p> <p>2、重保值守：由用户指定在特定的高风险时期，如重大活动、节假日或系统升级期间，由专业安全团队提供的加强型安全监控和管理服务，以防止和减少安全事件的发生。</p>
交付物	《日常值守报告》

## 3、网络安全等级保护测评服务

指标项	指标要求
期限频率	测评工作需在 90 个自然日内完成
服务范围	政务云上教育局及直属单位的两个自建系统（均为等保二级）
服务内容	系统等保二级复测

交付物	《信息系统安全等级保护测评报告》 《信息系统安全整改建议》
-----	----------------------------------

#### 4、网络安全培训

技术指标	指标要求
期限频率	一年 1 次
服务内容	一年 1 次（时间 1 天）全市教育系统网络管理员，线下集中培训，培训人数上限 100 人，开展网络安全及应急演练培训，提升相关人员网络安全意识、拓宽网络安全视野，同时检验应急预案适用性、应急机制科学性、应急体制合理性，通过事后总结分析，对应急预案不足之处进行修订，有效提升信息安全保障水平，不断培养信息化相关人员的网络安全应急处置能力和防护水平。 服务内容围绕网络数据安全法律法规，网络安全等级保护，人工智能在教育领域的应用、面临的风险及治理，安全事件应急演练培训等。
▲服务要求	至少提供 2 名专家级讲师，一名为网络安全资深培训师（相关网络安全知识、人工智能、应急演练等培训），另一名讲师为省市级相关网络安全职能部门负责人或高校网络安全专业方面专家（人员也可由甲方邀请，产生的相关费用由中标方支付）。
项目交付	培训 PPT 等

#### ▲三、供应商资格要求

- 1、法人或其他组织的营业执照等证明文件，自然人投标的须提供身份证明；
- 2、提供法定代表人身份证明书；
- 3、提供法定代表人授权委托书(委托授权代理人时必须提交)；
- 4、参加采购活动前 3 年内在经营活动中没有重大违法记录的书面声明；(格式自拟)
- 5、投标人须提供承诺函，承诺提供的服务满足询价通知书规定的技术/服务要求，如发现虚假参数中标行为，经查实后取消其中标资格，并按相关要求赔偿采购方相关损失。（格式自拟）
- 6、投标人须具有 ISO9001 质量管理体系认证、ISO27001 信息安全管理体  
系认证、ISO/IEC 20000-1:2018 信息技术服务管理体系认证证书（提供证

书复印件)

7、为确保服务能顺利推进，投标人拟派的项目负责人需同时具有信息系统项目管理师、系统集成项目管理工程师证书，技术负责人需同时具有信息安全工程师和 CISP 认证证书，中标后须提供相关有效资质证书复印件并加盖公章。

#### 四、定标原则

- 1、坚持公平、公正、公开选定的原则。
- 2、通过供应商资格性要求，且按报价最低原则确定成交供应商。

#### 五、采购单位联系方式

联系人：夏老师，电话：13957231902，地址：舟山市新城长升路 228 号舟山市教育服务中心。

舟山市教育服务中心

(盖章)

2025 年 6 月 5 日