南昌市工业和信息化局网络与数据安全支撑服务项目采购公告

一、项目基本信息

1.项目名称：南昌市工业和信息化局网络与数据安全支撑服务项目

2.采购预算：人民币 3 万元以内（含税）

3.服务周期：一年

4.采购方式：江西省网上中介服务超市竞价

5.服务范围：采购人机关单位所属业务信息系统、网络设备、办公终端设备等数据信息资产安全支撑保障。

二、采购服务内容

（一）漏洞扫描、渗透测试服务

1.漏洞检测：开展不少于四次全面的网络安全漏洞检测，覆盖本单位业务信息系统应用端口、服务器、办公终端、网络设备等全部数据信息资产，重点排查高危、中危安全漏洞、系统弱口令、安全配置不当等风险问题，出具《漏洞检测报告》，建立漏洞整改闭环台账，确保安全隐患整改到位。

2.渗透测试：在不影响系统正常运行的前提下，对本单位业务信息系统开展不少于四次全面的合规性渗透测试，采用模拟攻防手段挖掘系统隐性安全漏洞、权限管控缺陷、数据传输风险等深层隐患，检测政务云环境下系统权限安全、数据传输安全、云

资源配置安全、接口安全、日志安全等内容，出具《渗透测试报告》，针对中高危风险制定专项安全加固方案，完成隐患整改、复测验证。

（二）网络安全事件应急演练服务

组织一次全员网络安全应急演练，针对政务机关单位常见的网络攻击、数据泄露、病毒入侵、系统异常、办公终端中毒等安全事件制定演练方案，组织机关工作人员实操演练，提升单位全员应急处置能力。

（三）网络与数据安全培训服务

组织两次机关工作人员网络安全专题培训，培训内容贴合政务机关单位工作场景，涵盖网络安全规范、办公终端安全、数据保密、网络钓鱼防范、日常运维安全等内容，提升全员网络安全意识。

三、供应商资格要求

1.具备独立法人资格，营业执照经营范围包含网络安全、信息安全服务、信息技术咨询等相关内容，符合《政府采购法》相关资格要求条件。

2.近 3 年内无政府采购严重违法失信行为记录、无网络安全行政执法处罚记录、无网信部门安全通报问题及重大安全服务事故，可自行提供信用自查承诺函，一经查实弄虚作假，自动丧失参选及履约资格。

3.具备成熟的政务网络安全服务支撑能力，配备固定专职安

全服务工程师，持有CISP等国家级网络安全专业证书。

4.熟练掌握国家及江西省最新数字政府安全、政务数据分类分级、网络安全常态化督查相关政策标准，具备机关事业单位同类网络安全常态化支撑服务案例者优先。

5.不接受联合体参与，严禁服务转包、违法分包、挂靠服务，一经发现存在上述违规行为，立即取消服务资格、终止合同。

四、服务交付要求

1.漏洞扫描报告、整改复核台账;

2.渗透测试报告、安全加固方案;

3.网络安全应急演练全套方案及总结资料;

4.网络与数据安全培训全套方案及总结资料;

5.网络与数据安全服务工作总结报告、安全隐患整改闭环台账。

五、服务响应要求

1.日常问题7×24小时线上响应，工作时段紧急安全事件1小时内响应、4小时内出具处置方案。

2.配合采购人完成各级网络安全检查、数据安全督查、专项审计工作。重要时期，人员可根据实际需要驻点响应，协助采购人完成安全问题闭环整改，提供技术咨询、合规指导、隐患排查支撑，高效处置各类安全问题。

六、报价要求

本项目为总价包干报价，包含人工、培训、检测、工具、报告、差旅、税费等所有费用，采购人不再额外支付任何费用，超预算报价视为无效报价。