

# 南京紫金投资集团互联网信息系统 安全检测服务项目综合比选公告

为保障南京紫金投资集团（以下简称“集团”）数字化转型工作顺利推进，防范集团网络与数据安全风险，提升集团整体网络与数据安全水平，落实网络安全工作责任制，强化主体责任、属地责任，集团拟对集团及下属各子公司互联网信息系统开展一轮安全技术检测工作。现对集团互联网信息系统安全检测服务项目进行公开比选，有关事宜公告如下：

## 一、服务内容

1、互联网 IP 地址端口探测：检查开放在互联网侧的 IP 端口，对比资产清单，发现未知端口暴露情况。

2、网络安全漏洞扫描：利用漏洞检测工具检查系统可能存在的漏洞，并对漏洞进行人工验证。

3、网络安全渗透测试：利用已掌握的漏洞信息，模拟黑客攻击开展进一步人工测试，发现有威胁的风险漏洞。

4、弱口令检查：检查各业务系统是否存在弱口令情况。

5、数据安全渗透测试：模拟黑客攻击业务系统外部交互入口、数据接口 API 等，检查重要数据是否存在可绕过身份验证可超范围访问、可下载、可修改、可删除等数据安全权限风险。

6、敏感数据泄露互联网检测：检查互联网上是否存在与本单位相关的数据泄露、代码泄露、文档泄露等。

7、数据泄露风险检测：对系统用户账号与权限安全风险进行



检查，检测内容包括：多人共享账号、一人使用多账号、开放权限过大、账户越权操作、僵尸账号、非正常账号权限、数据共享管理缺失、账号权限独立性、权限滥用等。

8、APP 安全检测：对 APP 自身安全（病毒信息、权限信息、行为信息、敏感词检测、第三方 SDK 等）、程序源文件安全组件安全、用户操作安全、通信数据传输安全、本地数据存储安全、恶意风险防护安全等进行检查。

9、小程序安全检测：对小程序前端和后台 WEB 端检查，覆盖前台代码安全和 API 使用规范，以及业务 CG 和对 WEB 框架的安全检测。检测范围包括：配置管理测试、认证测试、会话管理测试、授权测试、数据验证测试、阻断服务测试、WEB 服务测试、AJAX 测试等。

10、APP/公众号渗透测试：对 APP 和公众号，模拟黑客攻击，对 APP 客户端、公众号等业务系统以及对应的服务端进行渗透性测试，测试范围包括：业务逻辑安全、后台服务端接口安全、身份鉴别安全、数据资源访问控制、组件配置安全、WEB 框架安全等。

11、APP/小程序（安卓）隐私合规评估：检查 APP/小程序隐私政策收集使用个人信息行为等是否合规。

12、网络与数据安全培训：提供网络与数据安全相关意识类培训、软件开发安全培训等。

13、网络与数据安全应急演练：提供一次网络与数据安全应



急演练工作。

14、驻场服务：服务周期内提供 2 人驻场，开展安全技术检测、应急相应、事件处置等安全服务。

以上服务内容完成后须输出相应的检测报告或服务报告。

## 二、服务对象

南京紫金投资集团本部及下属各级子公司所有互联网信息资产，包含各类应用系统、互联网接口、APP、小程序、IP 地址等不少于 109 个。

## 三、服务周期

服务总周期为 3 个月，其中安全技术检测时长至少 1 个月。

## 四、参选单位条件

(1) 参选单位必须在中华人民共和国境内依法注册并成立 3 年以上（截至开标日）的独立法人，且注册资本及实缴资本不少于人民币 500 万元，提供营业执照复印件及其他有效证明材料；

(2) 参选单位财务核算规范，具有良好的财务状况和经济活动，提供 2023 年度经会计师事务所审计的“无保留意见”会计报告完整版有效复印件（包括：资产负债表、利润表、现金流量表和财务报表附注）；

(3) 参选单位具有依法缴纳税收和社会保障资金的良好记录，提供 2022 年度或 2023 年度全年的（1 月至 12 月所有月份）“增值税”完税证明、近 6 个月内任意一个月的社保机构出具的参选单位社保缴费清单材料，社保材料必须为参保证明（加盖社

保部门有效印章)或缴纳证明(加盖税务部门或社保部门有效印章);

(5) 参选单位未处于被责令停业、响应资格被取消或者财产被接管、冻结和破产状态,企业没有因骗取中标或者严重违约以及发生重大违法违纪等问题,被有关部门暂停投标资格并在暂停期内;本项目不接受联合体(含关联关系的企业)响应及未经采购人同意的任何形式的转包、分包(提供承诺书,格式自拟,加盖公章);

(6) 截至响应截止日,参选单位未被“信用中国”网站(<http://www.creditchina.gov.cn>)列入失信被执行人、税收违法黑名单、政府采购严重违法失信行为记录名单(提供官方网站截图);

(7) 法定代表人为同一个人的两个及两个以上法人,母公司与全资子公司/由其控股的子公司,不得同时参与本项目(提供承诺书,格式自拟,加盖公章);

(8) 参选单位必须为增值税一般纳税人,提供一般纳税人证明材料;

(9) 参选单位须具有有效的 CCRC 信息安全服务资质认证证书

(10) 参选单位须具备国家级漏洞技术支撑单位或成员单位资质

(11) 参选单位须具备国家级 CNCERT 网络安全应急服务支撑单位资质

(12) 参选单位须具备江苏省、市级监管单位网络安全相关技术支撑单位资质

## 五、参选文件主要内容

(1) 参选单位简介（含公司介绍、营业执照、财务信息、税务信息、信用信息、相关资质证明等）

(2) 参选单位的服务解决方案（须针对采购人提出的服务内容做出详细、合理、全面的方案应答）

(3) 参选单位自 2021 年 1 月 1 日到投标截止日前（以合同签订时间为准）实施的国有企业类似项目案例，（合同内容需有“安全检测”或“安全技术检测”或“安全测试”或“渗透测试”或“人工渗透”或“安全渗透”或“安全评估”或“安全风险评估”或“安全服务”或“风险评估”关键词）

(4) 参选单位服务团队情况（项目负责人 1 人，须在本单位工作年限不少于 3 年，具备信息安全认证类证书和高级专业技术资格证书，驻场服务人员 2 人，须从事网络安全行业不少于 3 年，具备项目管理类和信息安全认证类证书，项目其他成员不少于 4 人，具备信息安全认证类证书或者安全测试类证书，提供有效证书复印件和社保证明材料），其中项目主要负责人不得随意替换，如有特殊情况，须书面报备我集团，否则视为违约。

(5) 参选单位承诺已充分理解采购需求，可按项目的采购



需求提供服务（提供承诺书，格式自拟，加盖公章）。

（6）报价明细单，加盖公章。

（7）其他相关资料

## 六、参选要求

（1）服务费用报价最高不得超过人民币 30 万元（含税）。

（2）参选单位必须真实、准确、完整的编制参选文件。

（3）参选单位应就项目提供参选文件一式五份（正本壹份，副本肆份，标注正副本），由参选单位的法定代表人或授权代理人签署并加盖公章，授权签署的需附授权委托书。

（4）参选单位须于 2024 年 5 月 24 日 14:00 前将参选文件（一式三份，标注正副本）密封并在封口处加盖公章，在密封袋上注明参选单位名称、联系人、联系电话和参选项目名称，邮寄或送达南京市雨花台区玉兰路 8 号国资大厦 318 办公室；

（5）参选文件送达后不可修改或撤回，采购人不负责参选单位准备文件、递交文件、参加报价所发生的任何成本和费用。

## 七、评选

我集团组织相关部门人员组成评审小组，对参选单位综合情况、服务方案、服务团队情况、典型案例、参选文件编制等进行逐项打分，该部分得分占比 65%，项目报价得分占比 35%，加总两部分得分最终确定成交供应商。

## 八、监督部门

本项目的监督部门为南京紫金投资集团有限责任公司。

九、联系方式

联系人： 熊伟

联系电话： 13901585203

联系邮箱： xiongw@zjholdings.cn

地址： 南京市雨花台区玉兰路 8 号国资大厦数字金融部

南京紫金投资集团有限责任公司

2024 年 5 月 21 日