**采购需求**

**一、采购项目概况**

1.为进一步提高我司信息系统的保障能力，根据《中华人民共和国网络安全法》（[主席令第53号](https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%BB%E5%B8%AD%E4%BB%A4%EF%BC%88%E7%AC%AC%E4%BA%94%E5%8D%81%E4%B8%89%E5%8F%B7%EF%BC%89/23119921)）、《国家网络安全事件应急预案》（中央网信办〔2017〕4号）、《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》等相关法律法规要求和安徽省信息系统网络安全等级保护相关要求，“合肥市卫星导航定位基准服务”（移动专网）、“合肥市测绘设计研究院综合业务平台”（含“EPS测绘地理信息一体化生产平台”、“泽塔云算力平台”、“房产测绘信息系统”等内网业务系统）和公司门户网站（外网）需依据等级保护2.0相关要求开展等保测评工作。

**二、采购目标**

依据公司的网络安全与信息安全现状和需求，完成对“合肥市卫星导航定位基准服务”（移动专网）、“合肥市测绘设计研究院综合业务平台”（含“EPS测绘地理信息一体化生产平台”、“泽塔云算力平台”、“房产测绘信息系统”等内网业务系统）和公司门户网站（外网）进行二级的等级保护测评，确保公司的网络和信息重要安全能够满足监管合规的要求。测评单位需依据相应等级的安全保护测评要求及测绘行业的特殊安全需求，对我司的信息系统网络安全进行等级保护符合性测评。测评内容涵盖物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、数据安全与备份恢复、安全策略和管理制度、安全管理机构和人员、系统建设管理、系统运维管理等信息安全的各个层面。

**三、资质/资格条件**

申请人的资格要求：

（1）资质要求：

①具有独立企业法人资格及有效的营业执照；

②具有有效的网络安全等级测评与检测评估机构服务认证证书和国家互联网应急中心颁发的“网络安全能力认证”培训机构证书。

1. 人员要求：

拟派技术团队（项目负责人1人，其他技术人员不少于3人）其中至少一人具有中级测评师资质，且具有中国信息安全测评中心颁发的“注册应急响应专家（CISP-IRS）”证书。

注：提供人员证书扫描件和2024年5月至今任意连续6个月的社保证明材料。

1. 业绩要求：

①供应商提供近二年内，已完成的具备党政机关（事业单位）或国有企业委托的信息系统等级保护测评服务业绩（以合同签订时间为准）。

②项目负责人至少独立承担过一次自2023年7月1日（含）以来已完成的类似测评项目的业绩。

（4）信誉最低要求：

①在国家企业信用信息公示系统（http://www.gsxt.gov.cn）中未被列入严重违法失信企业名单；

②在“中国执行信息公开网”网站（http://zxgk.court.gov.cn/index.jsp）中未被列入失信被执行人名单；

**四、实施原则**

**1.保密原则。**对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究中标人的责任。

**2.标准性原则。**测评方案的设计与实施应依据国家等级保护的相关标准进行。

**3.规范性原则。**中标人的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

**4.可控性原则。**测评服务的进度要跟上进度表的安排，保证招标人对于测评工作的可控性。

**5.整体性原则。**测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

**6.最小影响原则。**测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**五、项目需求**

**1.等级保护测评服务主要需求如下**

|  |  |  |  |
| --- | --- | --- | --- |
| **系统名称** | **等级** | **等保测评** | **备注** |
| 合肥市卫星导航定位基准服务 | 二级 | √ | 协助取得系统备案证明 |
| 合肥市测绘设计研究院综合业务平台（含“EPS测绘地理信息一体化生产平台”、“泽塔云算力平台”、“房产测绘信息系统”等内网业务系统） |
| 公司门户网站（外网） |

以国家等级保护相关标准《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》、《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》为基础，对采购人整体信息系统的构成、应用情况、网络结构、安全现状加以分析研究、编制信息系统测评技术方案和实施方案，提交差距分析、问题清单及整改意见、测评报告、等一系列技术文档。

**2.技术规格和标准**

（1）《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

（2）《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

（3）《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

（4）《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

（5）《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2020）

（6）《信息安全技术 网络基础安全技术要求》（GB/T 20270-2006）

（7）《信息安全技术 信息系统通用安全技术要求》（GB/T 20271-2006）

（8）《信息安全技术 操作系统安全技术要求》（GB/T 20272-2006）

（9）《信息安全技术 数据库管理系统安全技术要求》（GB/T 20273-2006）

（10）《信息安全技术 应用系统安全等级保护通用技术指南》（GA/T 711-2007）

（11）《信息安全技术 服务器技术要求》（GB/T 21028-2007）

（12）《信息安全技术 终端计算机系统安全等级技术要求》（GA/T 671-2006）

（13）《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

（14）《信息安全技术 信息系统安全工程管理要求》（GB/T 20282-2006）

（15）《信息安全技术 信息安全事件分类分级指南》（GB/Z 20986-2007）

**3.项目内容**

（1）漏洞扫描。供应商需针对网络设备，服务器，应用等进行漏洞扫描出具漏洞扫描报告。

（2）渗透测试。模拟黑客可能使用的攻击技术和漏洞发现技术，对信息系统进行验证性渗透测试。

（3）系统定级与备案。协助我单位完成系统的定级（含专家评审）与备案工作，最终取得公安部门下发的备案证明。

（4）等级保护测评。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 网络安全等级保护测评要求》（GB/T 28448-2019）等国家等级保护相关标准，参照《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018），完成安全技术层面包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全测评；安全管理层面包括安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。完成上述测评工作和整改加固实施后，供应商最后出具符合公安机关要求的各信息系统网络安全等级保护测评报告。

**4.测评结果反馈**

|  |  |
| --- | --- |
| **等级保护测评工作** | 1.问题清单及整改建议。  2.信息系统网络安全等级保护测评报告。 |

**5.采购标的的验收标准、付款方式**

1.验收标准：中标供应商在合同签订后的45天内完成测评服务内容，出具符合公安机关要求的（年度）信息系统安全保护等级测评报告。

2.付款方式：本项目合同签订后，中标供应商须向采购方提供符合要求的等额发票，票至付款。

**六、评定标准**

最低价优先。