单位名称（公章）：

联系人及联系方式：

**一、项目名称：**安徽建筑大学网站内容安全监测系统

**二、预算金额：**6万元，服务期为一年，服务期满后，经考核合格后，双方无异议可续签合同，最多续签两年，合同一年一签。

**三、项目概况：**

本次采购的网站内容安全监测系统，能够实现实时对安徽建筑大学目标网站进行内容监测和数据巡查预警。监测其内容是否存在不良、敏感信息；实时监测网站、站群是否存在外链、暗链、篡改、可用性、劫持、未知威胁等安全风险；实时监测网站敏感信息，监测政府网站是否泄漏国家密级信息；实时监测网站链接安全性筛查、境外IP链接筛查、无效地址诊断、页面关联分析。

**四、付款方式**

验收完成后一次性付款。

**五、服务范围及要求**

**（一）服务范围**
项目内容为安徽建筑大学网站内容安全监测的保障服

务，涉及学校主站及二类网站，服务范围为全校。

1. **服务总体要求**

项目采购内容主要是内容安全监测以及人工审核取证

服务。

1.内容安全监测

对业务系统网站站点进行全面而彻底的数据巡查和预警，具体建设内容如下：

（1）内容监测

对监测目标内容进行监测，通过敏感词库匹配，对涉政、涉黄、涉赌、涉暴恐、博彩等敏感词进行监测识别，支持自定义敏感词库及错别字词库设置。

（2）外链监测

对监测目标内容进行监测，通过对源代码中的超链接进行筛选、校验、分析，对网站可进行外链监测，监测网站是否被嵌入外链，发现网页中外链。

（3）自建敏感词库监测

内建百万级敏感词库收录、违规标签，覆盖涉政、涉黄、暴恐、违法违规、不良价值观、领导人、英雄烈士、邪教迷信、敏感专项、旗帜党徽、信息诈骗、社工欺诈、恶意文件等，监测维度包括：文字、图片、声音、视频共4个维度；

（4）反共监测

支持通过网络爬虫技术对境外反共黑客攻击篡改网站事件信息发布网站进行采集获取。

（5）涉党文献语录识别

关于国家领导人的讲话摘录、党的文献、国家政策等长语句进行校对，识别漏字、错字、语句不统一等问题。

（6）同音字错误识别

自动对同音但是字不同的文本进行识别，并提供改进意见。

（7）敏感词可视化定位

在页面及源代码中标红闪烁显示错误所在位置，高亮纠错。

（8）暗链监测

通过机器学习等算法，对监测目标进行暗链监测，对源代码中超链接进行筛选、校验、分析，监测监测目标是否被嵌入暗链，发现网页中错链、坏链、异常友链。

（9）篡改监测

基于自研的监测引擎提供扫描网页的篡改监控服务，通过远程实时监测目标网站页面的信息，采用对比技术与内容特征分析技术，如发现增加JS脚本、插入未知窗口、嵌入未知动画或增加未知内容等篡改行为，实时告警。

（10）劫持监测

通过对网站进行网页内容劫持等监测，提前做好网站防护工作，有效预防以及规避网站被劫持风险。

（11）未知威胁监测

可监测通过网页访问进入网站的未知病毒及恶意软件，提前做好网站防护工作，有效预防以及规避网站被未知威胁带来的风险。

（12）统计查询功能

支持按日、按周查询不良信息。支持批量导出不良信息，主要包含：违规域名、违规URL、内链/外链、违规信息类型、违规摘要、举证存放链接、网站名称、网站备案号、网站所有者、解析指向的IP地址、IP地址归属、整改建议等信息。

2.非法攻击监测

能有效防止SQL注入、异常HTTP请求、Webshell后门请求、XSS跨站脚本、命令执行、代码执行、文件包含、文件注入、防篡改、防盗链、防扫描等Web攻击。要求具备安全漏洞平台的计算机软件著作权证书，提供证书扫描件或影印件。

支持查看总攻击次数以及各种攻击类型的攻击次数。攻击类型包括：恶意扫描、XSS跨站、敏感文件访问、代码执行、文件包含、CC攻击、远程命令、SQL注入、Webshell、恶意采集、特殊攻击等。提供基于日志分析的CC攻击识别方法和设备的证书复印件或扫描件或影印件。

3.端口防护

要求能够对防护网站的非80端口可以自助配置,所有支持的http协议防护端口大于300个；https协议防护端口大于100个，提供管理平台自助设置的截图证明。

4.人工审核取证

主要包含人工审核取证服务，系统将审计任务自动分配给后台审计人员，不同审计人员分配不同的审计记录，具备人工初审、复审功能。支持图片、文本、视频二级审核和质检，可查看不良结果列表和系统处理记录，并进行质检与打标，打标完成形成算法识别训练素材。

同时， 对于本次项目工作，成立专门的项目服务小组，投入包括内容监测、产品支持、技术专项支撑与内容审核专家在内的技术力量。工作的具体情况如下：

（1）项目组人员情况

项目组共计7人：

包括内容监测运营人员2人、产品专项支撑1人、技术专项支撑1人、内容审核专家3人在内的技术力量。

（2）日常工作情况

具备技术运营支撑和巡检审核支撑；

周期性网站站点巡查，违规人审研判、取证告警；

专项培训：对以“二十大”、“建党百年”等类似关键事件节点进行专项培训和事件巡查。

5.其他

服务支持方式：正常的支持方式是通过电话、Email、远程终端进行；如校方提出需求，进行现场工作。

服务响应时间：正常情况下，每周一至周五，在接到故障申报后 4 小时内将提供故障处理的建议和方案。如周六周日遇重大问题，需配合接到故障申报后 6 小时内将提供故障处理的建议和方案。如果需要上门维护服务，将在 24 小时内提供远程或上门维修服务。

**（三）人员配备及服务要求**

1.投标人根据必须为本项目配备相关专业人员**（基本配备人员不少于 人）：【请各单位填写人员配备合理化建议】**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **职务** | **基本配备人数** | **注册证书** | **专业** | **等级** | **职称** |
| 1 |  |  |  |  |  | / |
| 2 |  |  |  |  |  | / |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **注：****1.人员必须分别设置，不得交叉任职。****2.投标文件中须提供为本项目配备上述人员的证书及2024年1月1日以来，投标人为上述人员缴纳的任意连续3个月的社保证明材料（任意险种），否则作无效标处理。** |

**2.投标人必须书面承诺，所配备的人员，能到现场服务，否则作无效标处理。投标人应根据项目情况，配备相关专业人员（填写人员配备表）。**

**（四）考核要求**

按照招标文件中要求开展的维保服务项目进行考核。

**六、商务部分调研【各单位请根据本单位实际情况填写】**

1.投标人综合实力

自2021年1月1日以来，获得具有中国信息通信研究院颁发的云分发服务资质证书 个；获得中国信息通信研究院颁发的内容审核服务系统测试证书 个；投标人获得具有公安部计算机信息系统安全产品质量监督检验中心或公安部信息安全产品检测中心出具的检验检测合格报告 个。

自2021年1月1日以来，投标人具备网络安全应急服务资质的：

国家级： 个；省级： 个；地市级： 个。

2.服务团队成员资质

售后服务技术人员资质证书，注册信息安全人员（CISP）证书 个；信息安全保障人员（CISAW） 个。

3.投标人业绩

自2021年1月1日以来，投标人具有网络安全或信息化（或网络）运维服务案例 个。

**七、其他方面的建议**