**附件1：**

**需求文件**

1. **服务内容需求:**

说明：

 服务要求表中标“**★**”系指本项目主要服务工作内容。

### 渗透测试服务

|  |  |  |
| --- | --- | --- |
| **服务类** | **技术类型** | **内容及要求** |
| 渗透测试 | 服务要求 | 1、成交供应商应保证采购人信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞，帮助采购人理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出有效的解决办法，切实保证信息系统安全。2、成交供应商应在得到客户授权后方可开始实施渗透工作。**★**3、成交供应商渗透测试人员应针对使用不同技术手段发现不同纬度的漏洞，同时提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度。 |
| 服务频率 | **★**提供含1个系统的高级渗透测试服务1次（需在2024年12月31日完成。） |
| 服务交付物 | **★**《渗透测试报告》、《渗透测试复测报告》 |
| 服务内容 | 广东省特种设备检测研究院江门检测院官网（www.jmsei.org.cn） |

### 漏洞扫描服务

|  |  |  |
| --- | --- | --- |
| **服务类** | **技术类型** | **内容及要求** |
| 漏洞扫描 | 服务要求 | **漏洞扫描应按照以下要求实施：** 1、成交供应商应对漏洞扫描结果进行人工验证，保证漏洞扫描结果的真实性。**★2、**成交供应商应针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。（提供漏洞修复方案样本，需包含多种修复方案以及修复过程中可能引发的其他问题的解决方案） |
| 服务工具要求 | ★1、成交供应商必须为保证所使用的所有工具和软件不会产生所有权和知识产权纠纷，并保证工具和软件的可用性和可靠性，成交供应商不是服务工具制造商的必须提供服务工具原厂商针对本项目的不存在知识产权纠纷及产品合格的书面证明函。由此产生的一切责任由投标人负完全责任。2、本项目使用的所有工具和软件（包括但不限于以下漏洞扫描工具、渗透测试工具）无需本项目采购方购买，均由成交供应商自行提供。**★3、**成交供应商须具备所使用漏扫工具制造厂商的合法授权**★4、**工具支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表。**★5、**按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。**★6、**支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。**★7、**支持导出统计报表和详细报告，统计报告包括综述信息、风险概况、资产风险列表、风险详情、参考标准、安全建议等内容；详细报告包括风险概述、资产风险列表、资产风险详情等内容，其中，基线风险会展示检测结果、风险等级、基线ID、基线项类型、风险值、检查点描述、解决方案等内容。漏洞风险会展示风险页面、风险等级、风险描述、危害影响、解决方案、参考资料、风险举证等内容。**★8、**支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级。**★9、**支持行业通用标准OWASP，支持通用WEB漏洞检测，如：SQL注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等。**★10、**提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。 |
| 服务频率 | **★**需在2024年12月31日完成 |
| 服务交付物 | **★**《漏洞扫描服务报告》、《漏洞复测报告》 |
| 服务内容 | 本单位内所有存在的IP设备漏洞扫描 |

### 应急演练

|  |  |
| --- | --- |
| **服务类** | **内容及要求** |
| 服务要求 | 成交供应商应帮助采购人通过应急演练最大限度地在安全事件发生前暴露预案和流程的缺陷，增强应对突发安全事件的信心和意识，提高队伍人员的熟练程度和技术水平成交供应商应结合采购人网络安全要求制定对应的应急演练预案，演练预案包含但不限于以下内容：* 有害程序事件：内网传播型病毒应急演练、勒索病毒应急演练、挖矿病毒应急演练等
* 网络攻击事件：漏洞攻击应急演练、后门攻击应急演练等
* 信息破坏事件：网站篡改应急演练、信息泄露应急演练等
* 设备设施故障事件：网络设备故障应急演练、服务器故障应急演练等

成交供应商根据采购人年度演练需求，参考演练预案制定演练方案，并提交至采购人相关人员进行评审成交供应商根据评审后的演练方案组织相关人员开展应急演练，并对应急演练过程进行记录，形成配套演练材料 |
| 服务频率 | ★1年内提供至少1次应急演练服务。（需在2024年12月31日完成。） |
| 服务交付物 | 交付文档：《应急演练脚本》、《安全应急演练方案》、《应急演练总结报告》 |

1. **供应商要求**

1、具备同类型至少3个项目经验，并提供相关证明文件。

2、需具备能规定时间完成项目的团队，且至少2人需拥有安全服务技术能力相关证书，并提供相关证明文件。

3、必须在2024年12月31号前出具所有有效报告和有效演练总结。（注：若在规定时间内不能交付所有有效报告，此项目为无效。）

1. **付款方式**

在到货并验收合格、需方收到供方开具的采购合同总价的发票后，需方在15个工作日内以支票或银行汇款（含电汇）的形式支付采购合同单总价款项

**附件2： 报 价 表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购内容** | **数量** | **报价****（人民币元）** | **备注** |
| 1 | 渗透服务、漏扫及应急演练服务 | 1 |  |  |

联系人： 联系电话：

**注：**

1. **供应商必须按报价表的格式填写，不得增加或删除表格内容。除单价、金额或项目要求填写的内容外，不得擅自改动报价表内容，否则将有可能影响成交结果，不推荐为成交候选人；**
2. **所有价格均系用人民币表示，单位为元，均为含税价；**
3. **平台上报价与报价表合计不一致的，以报价表合计（经价格核准后的价格）为准**
4. **报价表必须加盖单位公章，否则视为无效报价。**

供应商名称（单位盖公章）：

日期：

**附件3： 用户需求书响应声明函**

**致：广东省特种设备检测研究院江门检测院：**

关于贵单位、贵司发布渗透服务、漏扫及应急演练服务项目的招标公告，本公司（企业）愿意参加采购活动，并作出如下声明：

本公司（企业）承诺在报名时已对于用户需求书中的各项条款、内容及要求给予充分考虑，明确承诺对于本项目的用户需求中的各项条款、内容及要求均为完全响应，不存在任意一条负偏离或不响应的情况。本公司（企业）清楚，若对于用户需求书各项条款存在任意一条负偏离或不响应的情况，不被推荐为成交候选人的要求。

本公司（企业）承诺在本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

供应商名称（单位盖公章）：

日期：

## 附件4：承诺函

**致：广东省特种设备检测研究院江门检测院：**

关于贵单位、贵司发布渗透服务、漏扫及应急演练服务项目的招标公告，本公司（企业）愿意参加竞价，并承诺：

本公司（企业）在本项目中会随时进行技术支持。同时向用户提供免费安装服务，使其达到完全掌握系统的使用方法为止。

否则，由此所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

单位名称：

日期：