**附件**

## 信息安全等级保护测评服务项目需求

一、投标人资格要求：

1、符合《中华人民共和国政府采购法》第二十二条规定的供货商资格要求。

2、具有“网络安全等级测评与检测评估机构服务认证证书”资格

二、服务内容

本次等级测评的对象为以下信息系统，具体视实施过程中招标方需求明确：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **服务名称** | **系统等级** | **备注** |
| **1** | 绍兴仲裁院电子签名签 章系统信息安全等级保 护测评项目 | 二级 | 完成测评等工作 |

**等保测评**

三、依据标准

实施方应依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术网络安全等级保护测评要求

四、技术要求

根据国家网络安全等级保护相关标准，实施方对等级保护测评的内容包括但不限于以下内容：

安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据安全等五个方面的安全测评；

安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评；

**1、等级测评要求**

1)实施方应在对本单位系统详细了解的基础上，编制针对性的等级保护测评整体实施方案，包括项目概述、等级测评范围和内容、项目实施流程、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

2)实施方应详细描述测评人员的组成、资质及各自职责的划分。实施方应配置有经验的测评人员进行本次等级测评工作。

3)本次等级测评实施过程中所使用到的各种工具软件由实施方推荐，经采购方确认后由实施方提供并在测评中使用。在投标文件中应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

4)对于在测评过程中采用的测评方法、测评所使用的工具、测评所覆盖的各方面，需要符合信息安全等级保护主管部门要求，包括但不仅仅包括网络隐患检测工具、数据库漏洞检测工具、应用安全检测工具、网站安全检测工具等。

5)安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由实施方推荐，经采购方确认后由实施方提供并在测评中使用。

6)安全测评需要的运行环境（如场地、网络环境等）由采购方提供，实施方应详细描述需要的运行环境的具体要求。

7)项目完成后必须提交完整的技术文档、测评报告、整改建议等**。**

**2、项目实施要求**

1)实施方应保证投标项目在采购方条件成熟时应立即开展实施；

2)实施方在项目实施过程中应服从采购方的统一领导和协调，采购方有权裁决实施方的责任范围，实施方必须执行，在采购方限定的时间内解决问题。如果实施方不能按时完成测评内容，采购方有权中止项目、索赔或拒付款项；

3)实施方需根据自己的工程实施经验结合采购方的实际需求进一步细化和完善工作任务书，作为工程实施的指导性文件；

4)实施方应根据采购方工作需求、进度要求、实际情况制定详细的项目实施管理规范和项目实施计划，对工程目标、工作任务、阶段性工作、项目组织机构、职责分工、项目进度、质量控制等内容进行详细的说明，以确保工程实施按时保质的完成；

5)本次项目实施骨干人员至少包含1名高级测评师（提供证书复印件）。本项目负责人必须具有5年以上的测评工作经验，并参与过具有大型复杂测评项目的实施经验；承担本次项目的项目经理必须同时具有高级测评师、信息安全保障人员认证证书(CISAW)、国家重要信息系统保护人员培训证书（CIIPT）、信息安全管理系统审计认证（DNV）、商用密码应用安全性评估人员测评能力证书（合同签订时提供证书复印件，中标供应商不能提供的做废标处理）。

6)项目验收完成后，要求提供为期一年的安全咨询服务，以保证项目正常运行。

五、测评报告要求

实施方应对采购人的各个信息系统进行等级保护测评，形成相应的报告。

1)实施方在测评完成后，出具符合信息安全等级保护主管部门要求的信息系统安全等级保护测评报告；

2)对不符合信息安全等级保护有关管理规范和技术标准的，实施方出具可行的信息系统整改建议，并指导用户方完成整改；

3)实施方协助用户方办理信息系统安全等级保护备案手续等相关工作。

**源代码检测**

**一、服务目的**

检查[源代码](https://baike.baidu.com/item/%E6%BA%90%E4%BB%A3%E7%A0%81/3969%22%20%5Ct%20%22https%3A//baike.baidu.com/item/%E4%BB%A3%E7%A0%81%E5%AE%A1%E8%AE%A1/_blank)中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞。

**二、服务诉求**

当使用开源框架或开源插件等第三方集成代码时又或者代码中存在的一些其他隐患无法通过常规渗透测试检查出来，需要通过检查源代码来发现常规渗透无法发现的一些安全隐患。

**三、服务内容**

**1、代码的工具测试**

A)导入应用系统源码到测试环境

B)按预定代码安全策略对应用系统源码进行审计

C)过滤代码审计结果

D)将安全漏洞进行分组（按漏洞类型，按功能模块）

**2、人工检查**

1)根据人工审查手册，进行逐一人工审核

2)根据工具测试的结果进行分析，撰写相应的测试代码结合人工检查找出工具发现的安全漏洞中不确定和存在误报的漏洞

3)确认问题代码覆盖的范围，深入分析发现的安全漏洞

4)分析代码引用的资源文件

5)分析漏洞在当前系统中的严重等级（也可按不同的安全标准如：OWASP,PCI等）

**四、测试流程**

客户沟通——》逐行检测——》发现问题——》反馈客户——》整改复测——》编写报告

客户沟通：前期与客户沟通源代码事宜

逐行检测：逐行测试源代码安全风险

发现问题：发现问题后并分析问题成因提供整改建议

反馈客户：把问题和成因及整改建议反馈给客户

整改复测：整改完成后进行复测，直至安全

编写报告：问题整改完成即可编写报告