附件

项目说明和采购需求

一、项目概述：

为贯彻落实《中华人民共和国网络安全法》等国家法律政策中关于网络安全等级保护测评的工作要求，本次拟聘请具备技术能力的第三方机构，对宁夏计量质量检验检测研究院的OA办公自动化系统、业务信息系统进行网络安全等级保护测评工作。

二、服务目标：

1、完成宁夏计量质量检验检测研究院OA办公自动化系统、业务信息系统定级、备案的相关工作；

2、对完成定级备案的信息系统按照等保2.0相关要求开展信息系统网络安全等级保护测评工作出具测评报告，并对差距项提出整改建议。

3、提供网络安全培训服务 1次。

三、等级保护测评内容要求：

3.1 测评原则

等级保护测评实施方案设计与具体实施应满足以下原则：

3.1.1保密性原则：投标人应与采购人签订等级保护测评保密协议，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，不得利用此数据侵害采购人的权益，否则采购人有权追究投标人的责任。

3.1.2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。

3.1.3规范性原则：投标人工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

3.1.4可控性原则：测评服务的进度应符合进度安排，保证采购人对测评工作的可控性。

3.1.5整体性原则：测评的范围和内容应系统、全面、规范，满足国家等级保护相关基本要求。

3.1.6最小影响原则：技术测评工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评应在采购方许可的条件下进行。

3.2 测评依据

本次测评所有工作将完全遵循下述国家相关部门的标准和规范，以体现科学、客观、公正和高效的测评原则。

《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》

《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》

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

《GB/T 36627-2018信息安全技术 网络安全等级保护测试评估技术指南》

《GB/T 27070-2011信息安全技术 网络安全等级保护安全设计技术要求》

3.3测评的内容

测评的内容覆盖上述标准所要求的内容，包括但不限于以下内容：

安全技术测评：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、安全管理中心等五个方面的安全测评。

安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

3.3.1安全物理环境

根据信息系统机房和现场安全测评记录，针对机房和现场在“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等安全物理环境方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

3. 3.2安全通信网络

根据信息系统安全通信网络测评记录，针对通信网络方面在“网络架构”、“通信传输”、“可信验证””等方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

3. 3.3安全区域边界

安全区域边界现场测评包括“边界防护”、“访问控制”、“入侵防范”、“恶意代码和垃圾邮件防范”、“安全审计”、“可信验证”等边界区域防范措施进行检查。

3. 3.4安全计算环境

安全计算环境现场测评包括“身份鉴别”、“访问控制”、“安全审计”、“入侵防范”、“恶意代码防范”、“可信验证”、“数据完整性”、“数据保密性”、“数据备份恢复”、“剩余信息保护”、“个人信息保护”等几个方面的测评。

3. 3.5安全管理中心

安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中控制”等方面。

3. 3.6安全管理制度

根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

3. 3.7安全管理机构

根据现场安全测评记录，针对信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

3. 3.8安全管理人员

根据现场安全测评记录，针对信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

3. 3.9安全建设管理

根据现场安全测评记录，针对 信息系统在安全建设管理方面的“定级和备案”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、“外包软件开发”、“工程实施”、“测试验收”、“系统交付”、“等级测评”以及“服务供应商选择”等测评指标，判断出与其相对应的各测评项的测评结果。

3. 3.10安全运维管理

根据现场安全测评记录，针对 信息系统在安全运维管理方面的“环境管理”、“资产管理”、“介质管理”、“设备维护管理”、“漏洞和风险管理”、“网络和系统安全管理”、“恶意代码防范管理”、“配置管理”、“密码管理”、“变更管理”、“备份与恢复管理”、“安全事件处置”、“应急预案管理”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

通过现场测评，逐项找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，给出差距分析报告，并给出整改建议方案。待整改完毕后，进行结果确认，完成网络安全等级保护测评，出具测评报告，并将测评报告报当地公安机关备案。

3.4项目验收

验收应按照采购人确认的验收测试大纲进行，全过程必须由采购人在场见证。

 宁夏计质院信息系统等级保护测评项目目标是输出等级保护测评报告，该项目将产生一定数量的文档。协助宁夏计质院取得该年度的相关定级资质，并在公安局备案。

 投标人应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。

 投标人应提交验收流程、验收方法和验收依据。

 投标人应提供交付件归档办法和方式。

 投标人应提供详细的验收测试大纲或计划，大纲中应明确规定验收项目和必须满足的要求。大纲必须经采购人确认后方可生效。

 验收报告需双方代表签字认可。

3.5项目文档

投标人完成项目后应提供以下文档：

表3-1 投标人完成项目提供文档列表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **文档名称** | **提交时间** | **备注** |
| 1 | 《宁夏计质院信息系统安全等级保护测评整改建议》 | 合同签订后3周 |  |
| 2 | 《宁夏计质院信息系统安全等级保护测评报告》 | 完成现场测评后2周 |  |

四、质量保证：

投标人在等级保护测评方案设计、实施、验收的各个阶段，均应满足宁夏计质院信息系统正常稳定运行的要求。投标人出具的相关报告应得到等级保护行业主管单位认定。报告正本一式三份，采购人保留两份。

五、保密要求：

投标人承担被测评单位敏感信息的保密责任，在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。

未经双方书面同意，不得向第三方透露项目和涉及双方企业信息安全、技术成果的任何内容。

项目结束后，双方必须互相确认测评过程中提供的相关资料，相互承担保密责任。

六、其他要求：

1、开展信息安全等级保护测评工作的人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。

2、开展信息安全等级保护测评工作的人员应由参加公安部举办的信息安全等级保护测评人员培训、考试，并取得公安部信息安全等级保护评估中心颁发的等级测评师证书的人员组成。

3、项目投标报价应包含服务、人工、交通及税金等一切与本项目有关的费用，须完全达到采购人需求，采购人不再为本项目追加费用。

4、投标人须承诺如采购人在合同履行阶段对实施内容有相应调整，投标人须无条件配合，费用包括在本次投标报价之中，不得再追加费用。

5、付款方式：合同约定。