兰溪市人力资源和社会保障局网络安全

等级保护测评采购要求

**一、项目背景**

网络安全等级保护是国家关于信息安全的基本政策，《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号），明确要求我国信息安全保障工作实行等级保护制度，提出“抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。在2016年的第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》，为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，而制定的法律。由全国人民代表大会常务委员会于2016年11月7日发布，自2017年6月1日起施行。其中第二十一条也明确提出了“国家实行网络安全等级保护制度”，网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

**二、项目目标**

以信息系统的实际情况和现实问题为基础，遵照国家的法律法规和标准规范，参照国际的安全标准和最佳实践，依据相应等级信息系统的基本要求和安全目标，设计出等级化、符合系统特点、融管理和技术为一体的整体安全保障体系，完善信息系统的网络安全等级保护建设工作。

简单来讲就是根据等级保护基本要求对当前信息系统网络安全作一次全面的检查，形成测评报告，让信息技术主管部门对系统在网络安全方面作一个全面的了解，及时发现风险、漏洞所在，使单位信息化工作做到有的放矢，以增强单位信息系统抗风险能力。

|  |  |  |
| --- | --- | --- |
| **系统名称** | **级别** | **备注** |
| **社会保险综合管理系统** | **第三级** | **复测评** |

根据国家等级保护相关标准，投标人对上述的信息系统完成测评、报备等工作。要求对以上业务信息系统进行摸底、分析和梳理，提出测评方案。逐一对信息系统进行安全等级保护测评，信息系统安全等级保护测评的内容包括但不限于以下内容：

(1) 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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面的安全测评；

(2) 完成测评工作后，提出整改方案并实施整改，最后出具符合公安机关要求的信息系统安全保护等级测评报告，并协助上述系统单位完成信息系统安全保护等级备案工作。

**三、测评依据**

开展重要信息系统等级测评等服务，需遵循以下要求及标准：

1）中华人民共和国计算机信息系统安全保护条例（国务院第147号令）；

2） 关于开展全国重要信息系统安全等级保护定级工作的通知（公信安〔2007〕861号）；

3）信息安全等级保护管理办法(公通字[2007]43号）

4）信息系统安全等级保护定级指南（GB/T 22240-2008）；

5）信息系统安全等级保护基本要求(GB/T 22239-2019）；

6）信息系统安全等级保护测评要求(GB/T 28448-2019）；

7）《浙江省信息安全等级保护管理办法》。

**四、项目原则**

在本次项目实施过程中，项目团队应遵循以下原则：

1保密性原则

在体系优化工作开始前，与采购人签署保密协议，规定实施过程和实施结束后技术中心敏感信息的保密工作，如对数据加密存储、清除用户数据。

2最小影响原则

通过管理和技术两个层面将工作所带来的影响降至最小，避免由于占用技术中心过多人力或资源而干扰其正常业务，避免实施过程对信息系统的正常运行产生不利的影响。

3可操作性原则

通过详细定义每个阶段的任务和任务实践内容，明确定义参与人员的职责和每项工作开始前的必备条件和结束时的输出结果，从而规范实施的流程，保证实施过程的可操作性和可控性。

4质量控制原则

通过项目管理的方法，从项目的组织、角色定义与培训、沟通与确认、进度控制、文档控制、汇报与验收等多个环节保证评估服务的总体质量。

5风险规避原则

在体系优化工作开始前，充分考虑可能引入的多方面风险，告知用户可能存在的风险，并采取相应的控制措施加以规避。

6符合性原则

体系优化工作应符合国家、行业、国际等相关的安全标准与规范。

7整体性原则

体系优化的范围和内容应当系统性、全面，覆盖采购人安全所涉及的各个层面、业务条线、内部组织架构，力求建立全面、整体的安全防护体系。

**五、测评内容**

根据信息系统的安全保护等级，并依据《GB/T 22239-2019信息安全技术 信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》的条款要求，逐一对信息系统的安全保护等级进行测评，测评的内容包括但不限于以下内容：

(1)安全技术测评：包括安全物理环境、安全区域边界、安全计算环境、安全通信网络、安全管理中心五个方面的安全测评；

(2)安全管理测评：安全管理机构、安全管理制度、安全人员管理、安全建设管理和安全运维管理等五个方面的安全控制测评。

**六、测评要求**

1、投标人应详细描述本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、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、投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有经验的测评人员进行本次等级保护测评工作。

3、本次等级保护测评实施过程中所使用到的各种工具软件由投标人推荐，经采购人确认后由投标人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、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投标人推荐，经采购人确认后由投标人提供并在测评中使用。

5、安全测评需要的运行环境（如场地、网络环境等）由采购人提供，投标人应详细描述需要的运行环境的具体要求。

6、本项目负责人必须具有8年以上的测评工作经验，并参与过大型复杂测评项目的实施；必须同时具有高级测评师证书、高级信息系统项目管理师、高级网络攻防技术与信息安全应急响应、注册信息安全工程师CISP、高校兼职专业带头人相关证书，确保项目的顺利实施。

7、本项目技术负责人具有5年以上的测评工作经验的中级测评师，并同时具有注册信息安全专业人员(CISP)、云计算安全证书(CIIP-A)、信息系统项目管理师（高级）、国家专业技术人才知识更新工程培训证书，确保项目的顺利实施。

**七、项目验收**

本项目输出包括且不仅仅包括以下成果：

1、本项目输出包括且不仅仅包括以下成果：

* 《网络安全等级保护测评报告》
* 《网络安全等级整改建议书》

测评工作结束后，协助委托方完成系统的备案工作。

2、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。

3、投标人应提交验收方案，供招标人参考。

4、招标人将依据本项目的要求，组织相关部门或单位的技术专家对投标人提交的项目成果进行验收。

**八、保密要求**

1、投标人必须和采购人签订保密协议和非侵害性协议，投标人必须要与参加此次测评项目的所有项目组成员签订保密协议和非侵害性协议，在合同签订时一并提供给采购人。

2、投标人具体测评工作和等级保护测评报告的编写，必须在采购人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，投标人不得带离该地点。

3、投标人对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标人中标与否，其对上述内容的保密责任将长期存在。

**九、供应商要求**

1、符合政府采购法第二十二条：1）具有独立承担民事责任的能力；2）具有良好的商业信誉和健全的财务会计制度；3）具有履行合同所必需的设备和专业技术能力；4）有依法缴纳税收和社会保障资金的良好记录；5）参加政府采购活动前三年，在经营活动中没有重大违法记录及相关行业处罚记录；6）法律、行政法规规定的其他条件。

2、已获得国家网络安全等级保护工作协调小组办公室推荐的测评机构。

3、为“浙等保[2014]1号”文件中所列的测评机构。

4、具有ITSS信息技术服务标准证书、ISO9001质量体系认证证书、ISO27001信息安全管理体系认证证书的优先考虑。

5、具有政府部门认可的内网资产发现系统著作权证书、内网流量监控系统著作权证书、网站漏洞扫描系统著作权证书、服务器漏洞扫描系统著作权证书提供证书复印件优先考虑。