

附件：采购需求和评分标准

第一部分 采购需求

一、服务要求

本测评项目应依据《中华人民共和国网络安全法》、《信息安全技术网络安全等级保护定级指南》及相关法律法规及标准规范要求 and 海淀区智慧城市管理办法相关规定，对被评估系统进行等级保护三级测评，查找漏洞，找出差距，科学评价，提出具体、实用、有针对性的整改建议，并出具相关测评报告，协助采购人完成等保三级测评备案并通过验收。同时本测评项目需要满足海淀区对智慧城市管理办法中关于等保的相关要求，符合其规定。

二、服务原则

1. 保密原则：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，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任；签订合同时需一并签订保密协议书。

2. 标准性原则：测评方案的设计与实施应依据国家的相关标准进行；

3. 规范性原则：供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制

4. 可控性原则：服务的进度要按照招标文件的要求，保证采购方对于测评工作的可控性；

5. 整体性原则：服务的范围和内容应当整体全面，包括国家相关要求测评要求涉及各个层面；

6. 安全性原则：服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。

三、服务内容

1. 测评依据

根据《中华人民共和国网络安全法》和《信息安全技术网络安全等级保护定级指南》等标准要求，依法对信息系统进行等级保护测评工作。

主要根据标准和要求：

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字[2007]43号）

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

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

《信息安全技术信息系统安全等级保护实施指南》（GB/T 25058-2010）

《信息安全技术数据库管理系统安全评估准则》（GB/T 20009-2019）

2. 项目内容及技术要求

本次等保测评工作是对中国中医科学院西苑医院的海淀区中医服务体系建设项目(信息化部分)系统进行等级保护测评，旨在提高相关网络系统、主机系统和应用系统的安全性，保障被测信息系统的安全运行，达到网络安全等级保护标准。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、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

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。

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安全区域边界

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。

△④安全计算环境

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。

⑤安全管理中心

包括“系统管理”、“审计管理”、“安全管理”、“集中控制”等方面。

(2) 安全管理测评

包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的安全测评。

①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。

②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。

△④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。

⑤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。

(3) 提出整改方案

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，根据整改方案系统地进行整改。整改工作是对信息系统完善的过程，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。

(4) 等保测评报告

包括《信息系统网络安全等级保护测评方案》、《信息系统网络安全等级保护差距分析报告》、《信息系统网络安全等级保护测评报告》。等级保护测评报告需加盖测评专用章，内容必须满足当地公安机关备案要求，协助采购人通过等保三级测评。

五、成果交付

成交供应商应协助采购人通过等保三级的要求，提交的书面材料中包括但不限于以下内容：

《信息系统网络安全等级保护测评方案》

《信息系统网络安全等级保护差距分析报告》

《信息系统网络安全等级保护测评报告》

六、其他要求

1、工期要求

接到采购人通知后 2 个月内完成所有测评，服务期至本项目最终验收且通过等保三级测评。

2、保密要求

投标人应提供保密承诺书，严格履行保密义务，自签订合同之日起至服务期结束，采取必要的控制措施，防止因项目实施造成的任何信息泄漏。

第二部分：评分标准

评分因素	评分内容	满分
价格部分 10分	以满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分，其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×10%×100	10
商务部分 18分	1、投标人参与起草等级保护测评相关标准，每具备一个得1分，最多得5分。 2、投标人提供自2022年以来同类项目合同业绩，每提供1个合同得1分，最多得4分。	9
	1、投标人具有商用密码检测机构资质证书，得3分，否则得0分； 2、投标人具有中国网络安全审查认证和市场监管大数据中心颁发的信息安全服务资质认证证书（信息安全风险评估一级服务资质），得2分，否则得0分； 3 投标人具有中国软件评测中心颁发的“数据安全服务能力评定资格证书-数据安全评估二级”，得2分，否则得0分； 4 投标人具有 CCRC 信息安全服务资质（网络安全审计一级服务资质）证书，得2分，否则得0分； （注：需提供以上证书复印件并加盖供应商公章附于投标文件中，否则不作为得分依据）	9
技术部分	对项目需求和服务方案中的指标进行评价：完全满足招标要求得基本分15分，其中：带△的重要指标每存在一条负偏离扣2分，一般指标每存在一条负偏离扣1分，基本分扣完为止；如果一条中有多项指标出现偏离，只计算一次。	15
	根据项目情况及采购人要求，制订详细的进度与测评实施方案。根据投标人提供的方案详细性、合理性、可行性、措施针对性及与项目特点的符合程度进行综合评分： 1. 测评实施方案和进度方案详细，合理性、可行性、措施针对性强，得13-15分 2. 测评实施方案和进度方案基本可行，操作性较强，得9-12分； 3. 测评实施方案和进度方案合理性、操作性一般，得6-8分； 4. 测评实施方案和进度方案合理性、操作性不足，得3-5分； 5. 测评实施方案和进度方案不能满足采购需求或未提供，得0-2分。	15
	根据投标人提供的安全质量实施方案，从安全保证和质量保障措施等方面进行综合全面评审： 1. 安全质量实施方案合理可行，操作性强，得7-8分； 2. 安全质量实施方案基本可行，操作性较强，得5-6分； 3. 安全质量实施方案合理性、操作性一般，得3-4分； 4. 安全质量实施方案不能满足采购需求或未提供，得0-2分。	8

	<p>根据投标人提供的人员团队方案，从团队组织架构、团队人员配备、技术力量搭配、工作流程和岗位职责等方面进行综合评审。</p> <p>1. 人员团队方案合理可行，操作性强，得 7-8 分；</p> <p>2. 人员团队方案基本可行，操作性较强，得 5-6 分；</p> <p>3. 人员团队方案合理性、操作性一般，得 3-4 分；</p> <p>4. 人员团队方案不能满足采购需求或未提供，得 0-2 分。</p>	8
	<p>1. 项目经理同时具有网络安全等级保护测评师（高级）证书、商用密码应用安全性评估人员测评能力证书得 3 分；每具备注册信息 CISP 证书、注册信息安全认证专家 CISSP 证书、重要信息系统安全等级保护培训证书 CIIP 任意一个加 1 分。此项总分最多得 6 分；</p> <p>2. 项目核心团队成员同时具备网络安全等级保护测评师（高级及以上）、商用密码评估考核证书，每有一人得 1 分，此项最高得 6 分。</p> <p>3. 项目团队除项目经理和项目核心团队成员外，每具备信息系统项目管理师（高级）、信息安全保障 CISA、注册数据安全治理专业人员（CISP-DSG）、注册信息安全认证专家 CISSP 证书任意一个加 1 分，最多得 4 分；（备注：多人有同一种证书只计 1 分）</p>	16
服务部分	<p>对投标人提供的服务保障方案，从响应时间、服务方式、服务内容、服务保障、保密措施等方面进行评审：</p> <p>1. 服务保障方案合理可行，操作性强，得 8-10 分；</p> <p>2. 服务保障方案基本可行，操作性较强，得 5-7 分；</p> <p>3. 服务保障方案合理性、操作性一般，得 3-4 分；</p> <p>4. 服务保障方案不能满足采购需求或未提供，得 0-2 分。</p>	10

根据采购需求和评分标准自拟应答文件，正本 1 份，副本 2 份。供应商应将所有应答文件都密封包装。所有密封包装的封面上均应清楚注明：项目名称、供应商名称和地址。密封包装封面上需加盖供应商公章。