****

国药东风总医院**网络安全等级保护测评**

采购项目

采购文件

项目名称：国药东风总医院**网络安全等级保护测评**采购项目

项目编号：ZB-GYDFZYY-2023-10-0001

采购人：国药东风总医院

**2023年10月**

**第一章 采购书**

1. 项目名称：国药东风总医院**网络安全等级保护测评**采购项目

2. 项目概况：详见技术要求

3. 资金来源：自筹

4. 交货方式、地点：

运输方式：由报价人自行确定（包装费、运输费及保险费，包含在总报价内）

交货地点：湖北省十堰市大岭路16号

收货单位：国药东风总医院

5. 货款结算方式：

当年测评的信息系统，取得公安部门颁发的三级等保备案证书后，一次性支付等保测评费用。

6. 报名时间：2023年10月23日至2023年10月30日

7. 报价截止时间：2023年10月30日下午18：00以前

8. 评审时间：另行通知

9. 报价方式：纸质报价

10. 业主联系方式：

联系单位：国药东风总医院

联系人：陈静 电话： 13907280772

技术顾问：何永钢 电话： 18986911234

**国药东风总医院**

**2022年计算机采购项目**

**国药东风总医院**

**网络安全等级保护测评招标要求**

**一、资格要求**

1.供货商应具备《政府采购法》第二十二条规定的条件。

2.供应商必须是在中华人民共和国境内注册并取得营业执照的具有独立法人的合法企业。

3.供应商必须持有公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》（需在投标文件中附复印件）。投标人须具有本地化服务能力，非湖北区域内公司需提供湖北省网络安全等级保护工作协调小组办公室颁发的《等级测评机构异地测评项目备案表》、本地化分支机构证明材料和本地化常驻人员近一年的社保证明。

4.参与测评人员不少于4人，其中须提供至少一名高级测评师资格证明或测评人员具有CISP证书（种类含盖CISO、CISE和CISP-PTE等）；

5、本项目不允许联合体投标。

**二、项目概况**

1、项目名称：国药东风总医院网络安全等级保护测评

2、项目说明：协助完成两个拟定为三级的信息系统（数字化信息管理系统、医院信息集成平台）的安全等级保护定级、备案、测评、整改等工作。

**三、项目需求**

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 系统等级 |
| 1 | 数字化信息管理系统（包含HIS、LIS、PACS、EMR） | 三级 |
| 2 | 互联互通集成平台 | 三级 |

**1、定级备案服务**

完成被测信息系统定级、备案材料的编写工作，完成到公安监管等部门办理备案手续工作，确保信息系统安全保护等级定级准确、备案完整。

**2、信息系统等级测评**

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》、《GB/T 28448-2019 信息安全技术信息系统安全等级保护测评要求》、《GB/T 25070-2019信息安全技术网络安全等级保护安全设计技术要求》、《GBT28449-2018信息安全技术 网络安全等级保护测评过程指南》、《GB/T 20984-2007 信息安全技术信息安全风险评估规范》、《GB/T 22080-2008 信息技术安全技术信息安全管理体系要求》、《GB/T 22081-2008 信息技术安全技术信息安全管理实用规则》等标准的要求，对国药东风总医院进行等级测评，出具符合国家网络安全等级保护格式要求的等级测评报告。测评范围为项目目标所涉及的机房基础设施、网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度。服务目标为系统最终通过公安部门及相关部门的等级保护检查要求。

测评内容应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、安全计算环境和安全管理中心等五个方面的安全测评；

（2）安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；

**3、编制等级保护安全建设方案**

范围

本次安全建设设计方案应符合等级保护相关规定，具体包括物理安全措施，网络基础设施；安全基础设施；应用系统硬件、软件；安全策略；管理规范和流程；系统架构等对象。

工作内容

测评完成后根据测评结果并依据《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》、《信息系统安全保护实施指南》、《信息系统安全管理要求》、《信息系统通用安全技术要求》、《信息系统等级保护安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求制定信息系统信息安全等级保护建设方案。后续提供咨询服务，协助用户完善信息系统安全防护措施，使各信息系统达到等级保护基本符合的要求。

**4、标准和规范**

《中华人民共和国计算机信息系统安全保护条例》国务院[1994]147号

《关于加强信息安全保障工作的意见》中办发[2003]27号

《关于信息等级保护工作的实施意见》（公通字66号）

《信息安全等级保护管理办法》公通字[2007]43号

《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》 （发改高技[2008]2071号）

《计算机信息系统安全保护等级划分准则》(GB17859-1999)

《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2019)

《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240-2020)

《信息安全技术 信息系统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安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239-2008)

《信息安全技术 信息系统安全等级保护定级指南》(GB/T 22240-2008)

《信息安全技术 信息系统安全等级保护测评要求》(GB/T 28448-2012)

《信息安全技术 信息安全等级保护 信息系统物理安全技术要求》(GB/T 21052-2007)

《信息安全技术 信息系统安全等级保护实施指南》

《信息安全技术 信息系统安全等级保护测评准则》

《信息安全技术 信息系统通用安全技术要求》(GB/T20271-2006)

《信息安全技术 网络基础安全技术要求》(GB/T20270-2006)

《信息安全技术 操作系统安全技术要求》(GB/T20272-2006)

《信息安全技术 数据库管理系统安全技术要求》(GB/T20273-2006)、

《信息安全技术 服务器技术要求》

《信息安全技术 终端计算机系统安全等级技术要求》(GA/T671-2006)

《信息安全技术 信息系统安全管理要求》(GB/T20269-2006)

《信息安全技术 信息系统安全工程管理要求》(GB/T20282-2006)

《信息技术信息安全管理实用规则》（GB/T 19716-2005 ）

《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

**5、测评实施原则**

在项目实施过程中必须满足以下原则：

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招标方的行为。

标准性原则：测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。

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。

可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能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。

整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

**6、整体要求**

（1）供应商应提供本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2）供应商应提供测评人员的组成、资质及各自职责的划分。供应商应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

（3）投标人应详细描述测评人员的组成、资质。投标人参与测评人员不少于4人，必须提供至少一名高级测师资质证明或CISP证书种类涵盖CISO、CISE和CISP-PTE等。

（4）本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件应符合国家相关要求，经招标人确认后由供应商提供并在信息系统等级保护测评中使用。

（5）信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，供应商应详细描述需要的运行环境的具体要求。

**7、专用工具要求**

本项目涉及工程实施和验收测试所需的工具，由供应商负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

**8、安全管理要求**

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

(1)等级保护测评前

1）对等级保护测评人员要进行安全保密教育，制定安全保密措施；

2）签订安全保密协议。

(2)等级保护测评中

1）对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理；

2）等级保护测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序；

3）对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围；

4）对测评设备、介质进行严格的保密管理；

5）工作过程中对人员要实施封闭式集中管理；

6）对进场人员遵守被测单位的相关管理规定。

(3)等级保护测评后

1）认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏；

2）现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序；

3）在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

**9、文档要求**

文档或报告的编写应完整清晰、用词规范、简明扼要，指出的问题应明确合理、符合逻辑、且有证据，出具的结论应公正客观、实事求是，提出的建议应符合国家标准规范、富有建设性和可操作性。

**10、技术支持**

供应商应提供机构背景材料、等级保护测评专业资质及其他认为可以体现技术能力的资质。供应商应提供测评成员的技术背景资历资料、从事测评的经验、人力资源的组织方式、项目实施的管理方式、项目成员的角色和责任。

**11、售后服务**

1）供应商在湖北省内设有售后服务机构，可提供7\*24热线电话，提供技术支持，如解决不了，技术人员需在接到电话后4个小时内赶到现场。

2）供应商承诺能按要求实现本技术规范规定的所有条款及功能要求，配合完成相关政府部门的信息安全等级保护相关（登记、整改等）工作要求。

**12、项目实施内容与要求**

**12.1、项目定级备案**

投标方应梳理现有的信息系统，严格按照《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》的要求，对信息系统的级别进行划定。完成信息系统定级报告及定级材料的准备、整理，完成信息系统去公安机关的备案工作。

**12.2、项目测评内容**

根据国家等级保护相关标准《GBT22239-2019 网络安全等级保护基本要求》，对重要信息系统等级保护测评项目应包括以下内容：

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：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、安全运维管理等五个方面的安全测评。

服务内容：

1. 协助开展系统和重要信息系统的自查自评估工作，对存在的风险隐患和安全问题及时提供有针对性的安全整改建议，保障整改措施的落实，完成重要信息系统的定级、备案等相关工作；
2. 依据《网络安全等级保护基本要求》，从安全技术和管理两个方面共十个层面对信息系统进行等级测评，出具等级测评报告；
3. 针对信息系统等保测评实施过程中发现的安全隐患和薄弱环节，提供安全建设整改和安全加固方面的咨询。
4. 提供安全服务，及时发现信息系统中存在安全隐患和威胁，进一步开展安全建设整改工作，及时、有效、正确的预防和阻止各种黑客攻击。职责清晰，能快速及时的帮助客户处理网站安全事件。

|  |  |  |
| --- | --- | --- |
| **项目** | **服务内容** | **工作描述** |
| 等级测评 | 项目准备及现场调研 | 协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。 |
| 信息系统定级、备案 | 疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备；  整理、补充信息系统备案所有相关的文档，完成相应信息系统等级保护备案工作。 |
| 信息系统差距分析 | 对定级的信息系统，依照《网络安全等级保护基本要求》进行逐个对照，分析信息系统安全情况与等级保护基本要求的差距，完成信息系统等级保护差距分析报告。 |
| 等级保护安全整改 | 协助落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、辅助进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。 |
| 等级保护测评 | 参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。 |
| 成果 | 服务目标为：协助用户取得公安机关备案证明；通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》。 |

**12.3、测评要求**

（1）安全物理环境物理安全测评是对信息系统的机房和办公场所的物理位置选择、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、电磁防护等方面的安全状况。

（2）安全通信网络

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性测评、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

1. 安全区域边界

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

（4）安全计算环境

安全计算环境是对信息系统的身份鉴别、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、个人信息保护等方面的安全状况。

（5）安全管理中心

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

（6）安全管理制度

安全管理制度测评是对信息系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。

（7）安全管理机构

安全管理机构测评是对信息系统的岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等情况进行测评。

（8）安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗安全意识教育和培训、外部人员访问管理等情况进行测评。

（9）安全建设管理

系统建设管理测评是对信息系统建设过程中的、测试验收、系统交付、等级测评服务供应商管理等情况进行测评。

（10）安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、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、外包运维管理等情况进行测评。

* **4、测评风险规避要求**

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

（1）操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

（2）操作时间控制

* 对测评直接影响系统工作时，尽可能避开敏感时期。

（3）人员与数据管理

* 必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

（4）制定应急预案

* 根据测评范围界定的系统情况，在实施前制定应急预案。

（5）关键业务系统风险控制

* 对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

（6）优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

（7）数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

* **5、整改实施内容**

投标方严格按照差距分析报告内容，落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。

* **6、汇总项目材料并验收**

投标方对整改后的内容进行最终确认，并汇总信息系统等级保护测评报告，完成公安机关的材料报备，取得信息系统备案证明。

投标方汇总等级保护测评阶段性文档（不限于定级备案材料、差距分析报告、整改实施方案、测评报告、备案证明等），保证通过评审及验收。

**13、测评风险规避要求**

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点，按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

厂商协作

厂商需要提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在测评之前，由三方共同分析测评对业务可能造成的风险，分析可能存在的问题。在测评过程中尽量规避这些风险。

**四、其它要求**

1、如成交供应商发生兼并、重组，由新组建的公司按投标文件承担相应售后服务；

2、供应商使用的技术装备、设施应当符合《信息安全等级保护管理办法》中对信息安全产品的要求；

3、供应商的技术方案中应有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

**五、评标办法**

本次评标采取综合评分法，满分100分，由投标报价（30分）、技术（25分）、商务（45分）组成，最终得分=投标报价得分+技术得分+商务得分，具体细则见下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评审因素 | 分数 | 评分标准 |
| 报价部分（30分） | 最终磋商报价 | 30 | 1. 价格分统一采用低价优先法计算，即满足磋商文件要求且最后报价最低的供应商的价格为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算： 2. 投标报价得分＝（评标基准价/投标报价）×30%×100 3. 因落实政府采购政策进行价格调整的，以调整后的价格计算磋商基准价和磋商报价得分。 4. 评审小组认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在磋商现场合理的时间内提供书面说明，必要时提交相关证明材料。 |
| 商务部分（45分） | 体系认证证书 | 4 | 供应商具有相关部门颁发的ISO9001质量管理体系认证证书、ISO/IEC27001信息安全管理体系认证证书每项得2分，没有不得分，最高得4分。（须提供在有效期内的证书复印件并加盖供应商公章） |
| 6 | 供应商具有ISO27701隐私信息管理体系认证证书的得6分，否则不得分。（须提供在有效期内的证书复印件并加盖供应商公章） |
| 企业业绩 | 2 | 供应商提供近一年开展信息安全等级保护测评的相关案例，每提供一个得1分，最高得2分。（需提供合同复印件或中标通知书复印件，加盖供应商公章） |
|  | 6 | 供应商应具有设备设施保障能力，按要求完成等级保护测评工作   1. 供应商拥有公安部认可的等级保护测评工具箱得2分。(提供购买发票并加盖供应商公章） 2. 供应商拥有自主知识产权的测评工具或测评系统每个得0.5分，最高得2分。(提供软件著作权证明文件并加盖供应商公章） 3. 供应商拥有自主化研发团队得2分。(提供有效期内的CMMI软件能力成熟度三级资质并加盖供应商公章) |
| 企业资质 | 8 | 投标人拟投入的项目经理具备系统分析师、信息系统审计师ISA，以上证书每提供一个得4分，本项最高得8分，未提供不得分。（提供有效证书及人员社保证明并加盖供应商公章） |
| 8 | 投标人拟投入的技术负责人具备中级及以上测评师资质、CISP-CISE注册信息安全专业人员证书、CCSC网络安全能力认证证书，以上证书每提供一个得2分，若在信息安全专业刊物上发表过2篇及以上论文得2分，本项最高得8分，未提供不得分。（提供有效证书及人员社保证明并加盖供应商公章） |
| 6 | 为保证项目质量及售后服务，供应商应具备中国网络安全审查技术与认证中心（CCRC）出具的专业信息安全风险评估、安全审计，以上资质每提供一个得3分，本项最高得6分，未提供不得分。（须提供在有效期内的证书复印件并加盖供应商公章） |
| 技术  部分（30分） | 定级备案  及安全建设咨询服务 | 10 | 1. 在对应定级备案服务工作方案中：   承诺严格依据《网络安全等级保护定级指南》（GB/T 22240-2020）等技术标准要求，对信息系统开展信息系统调查、定级对象分析、定级要素分析、撰写定级报告，组织对信息系统定级进行专家评审，出具公安机关认可的专家评审意见，整理全套定级备案材料。完全满足以上要求，得5分，否则不得分。   1. 能按要求编制对应的安全整改建设方案：   测评完成后根据测评结果，依据《网络安全等级保护管理办法》、《网络安全等级保护基本要求》、《信息系统安全保护实施指南》等相关等级保护技术标准和管理规范要求，汇编信息系统安全管理制度，出具被测评信息系统《网络安全建设整改建议》，并协助采购方完成被测评信息系统的安全整改，完善信息系统安全防护措施，规划整体安全架构。完全满足以上要求，得5分，否则不得分。 |
| 安全等级  测评服务 | 10 | 1. 依据《网络安全等级保护基本要求》（GB/T 22239-2019）、《网络安全等级保护测评要求》（GB/T 28448-2019）、《网络安全等级保护测试评估技术指南》（GB/T 36627-2018）等政策法规和标准规范要求（如有新版标准，以新版为准），逐一对信息系统进行安全保护等级测评和评估，开展信息系统等级保护测评工作，测评目标包括服务内容所涵盖的系统。完全满足以上要求，得2分，否则不得分。 2. 测评范围为项目目标所涉及的机房基础设施、网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度等。完全满足以上要求，得2分，否则不得分。 3. 在响应文件中提供了编制安全等级测评工作方案和初步计划安排，且编制的测评工作方案和初步计划安排要求包含保障措施、进度计划目标承诺及惩罚措施，措施内容详细、切实可行、针对性强，每满足一项得1分，满分3分。 4. 按要求完成等级保护测评工作。承诺依据政策要求、技术标准和管理规范对各信息系统进行等级保护测评，主要包括以下内容：1）安全技术测评、2）安全管理测评、3）系统整体测评。 5. 承诺测评对象主要包括以下内容：1）物理环境部分、2）机房网络设备、3）机房安全设备、4）主机服务器部分、5）数据库部分、6）涉及到被测评的信息系统所有管理制度和相关记录证明文件、7）国家关于网络安全等级保护测评要求的其他内容。完全满足以上要求，得3分，否则不得分。 |
| 质量控制及保证措施 | 10 | 1. 测评实施中应对信息系统的正常运行不产生明显影响，提出了最小影响控制措施方案，方案内容准确详细、切实可行、针对性强，每满足一项得1分，满分3分。 2. 根据测评范围界定的系统情况，在实施前制定应急预案，内容详细、切实可行、针对性强，每满足一项得1分，满分3分。 3. 提出质量控制及保证措施方案，包含项目质量控制及保证措施，内容详细、切实可行、针对性强，每满足一项得1分，满分3分。 4. 承诺因供应商测评报告质量原因无法完成备案，测评机构无条件整改。提供加盖供应商单位公章的书面承诺，得2分，否则不得分。 |
| 1.总得分相同时确定排序的原则：以商务部分得分高的排名靠前；商务标仍相同的，以技术部分得分高的排名靠前。  2.磋商报价如果出现算术修正，并经供应商确认后，应以修正后的报价进行评审。  3.各供应商的最终得分计算方式为：  ☑各评委对其总评分的算术平均值  □各评委对其总评分去掉一个最高分和一个最低分后的算术平均值 | | | |

**一、供应商资质要求：**

3.1.1 供应商应是注册于中华人民共和国的独立企业法人，满足采购文件要求资格的企业；

3.1.2 符合政府采购法第二十二条规定的供应商资格条件：

①具有独立承担民事责任的能力；

②具有良好的服务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人员；

④具有依法缴纳税收和社会保障资金的良好记录；

⑤参加本次投标活动前三年内，在服务活动中没有重大违法记录；

⑥近三年内不存在违反招投标和政府采购相关法律法规的禁止行为；

**二、投标文件要求：**

1. 有效期内的营业执照正副本复印件
2. 投标文件真实性的声明函；
3. 投标代表为法人代表的，需提供法人代表证明书原件和法人代表身份证复印件；
4. 投标代表非法人代表的，需提供“法定代表人授权书”原件及投标代表本人身份证及复印件和法人身份证复印件；
5. 投标人符合规定条件的业绩；
6. 报价单（含税）。