成都市金牛区妇幼保健院

院内询价采购公告

一、项目名称：信息安全三级等级保护测评项目。

二、项目发布方式：

本项目在成都市金牛区妇幼保健院官网主页上公开发布（提供免费下载），供符合条件的生产企业、经营企业以及潜在供应商前来参加。

三、期限：

2022年4月21日-2022年4月25日。期间请各潜在供应商到我院院务部提交资料。

1. 项目要求：

（一）项目建设背景

为了落实公安部和卫健局应用系统安全等级保护要求，进一步增强系统安全防护能力，确保系统安全稳定运行，防止因系统安全事件引发安全事故依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全等级保护管理办法》（公通字[2007]43号）和《中华人民共和国网络安全法》等标准规范， 成都市金牛区妇幼保健院现拟招一家供应商提供等保测评服务。

（二）项目建设目标

依据国家和行业信息安全的相关标准，全面了解和掌握企业为系统现有安全状况，找出其与《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）对应级别的差距，及时发现系统存在的安全问题，针对等级保护测评中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。

（三）项目建设方案

依据《GBT 28448-2019信息安全技术 网络安全等级保护测评要求》，按照《信息安全技术 网络安全等级保护测评过程指南》GB-T 28449-2018要求，采取相应的测评方法（包括：访谈、检查、测试），按照相应的测评规程对测评对象（包括：制度文档、各类设备、安全配置、相关人员）进行相应力度（包括：广度、深度）的单元测评、整体测评，对测评发现的风险项进行分析评估，提出合理化整改建议，最终得到相应的信息系统等级测评报告。

（四）项目建设依据

此次依据的标准包括但不限于以下内容：

1）《中华人民共和国网络安全法》

2）《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019

3）《信息安全技术 网络安全等级保护定级指南》GB/T 22240-2018

4）《信息安全等级保护管理办法》（公通字[2007]43号）

5） 《四川省卫生健康行业网络安全等级保护工作实施方案》（川卫函〔2019〕11号）

6） 关于印发《省委巡视组反馈网络安全问题整改工作方案》的通知（川卫办信统便函〔2022〕6号）

（五）工作内容及要求

5.1测评对象

|  |  |
| --- | --- |
| 系统名称 | 安全等级 |
| HIS系统 | 三级 |
| 医院信息平台 | 三级 |

5.2 测评要求

根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：

| **序号** | **关键实施阶段** | **工作要求** |
| --- | --- | --- |
| 1 | 确定测评范围 | 明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。 |
| 2 | 获得信息系统的信息 | 通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。 |
| 3 | 确定具体的测评对象 | 初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。 |
| 4 | 确定测评工作的方法 | 根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。 |
| 5 | 制定测评工作计划 | 制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。 |
| 6 | 实施等级保护测评 | 实施测评，包括人工检查、工具扫描等方式。 |
| 7 | 项目总结 | 对测评结果进行总结、汇报 |

5.3 测评内容

按照信息系统等级保护测评依据开展测评工作（包括不限于以下项目）

5.3.1安全物理环境

安全物理环境检查主要是了解信息系统的物理安全保障情况，涉及对象为机房。在内容上，安全物理环境层面测评实施过程涉及的工作单元，具体如下表：

表1 安全物理环境测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 物理位置的选择 | 检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。 |
| 10 | 电磁防护 | 检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

5.3.2安全通信网络

安全通信网络检查主要是了解系统的网络架构和通信传输等，涉及对象为防火墙、核心路由器、核心交换机等设备和网络架构。在内容上，安全通信网络层面测评过程涉及的工作单元，具体如下表：

表2 安全通信网络测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 网络架构 | 检查核心设备的CPU和内存使用率，整个网络带宽是否满足现状，VLAN划分是否合理，网络架构是否做到设备冗余、链路。 |
| 2 | 通信传输 | 检查数据在传输过程中的的完整性和保密性措施。 |
| 3 | 可信计算 | 检查设备是否进行可信验证。 |

5.3.3安全区域边界

安全区域边界检查主要是了解系统在网络边界的防护措施，涉及对象为防火墙、入侵检测、安全审计等安全设备。在内容上，安全区域边界层面测评实施过程涉及的工作单元，具体如下表：

表3 安全区域边界测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 边界防护 | 检查网络边界是否有访问控制设备，访问控制策略是否合理，是否关闭了闲置端口等。 |
| 2 | 访问控制 | 检查网络中的访问控制策略是否合理、有效。 |
| 3 | 入侵防范 | 检查网络中是否采用了入侵防范措施，验证该措施是否有效。 |
| 4 | 恶意代码和垃圾邮件防范 | 检查网络中是否有恶意代码和垃圾邮件防范措施。 |
| 5 | 安全审计 | 检查网络中是否有综合安全审计措施。 |
| 6 | 可信验证 | 检查设备是否进行可信验证。 |

5.3.4安全计算环境

安全计算环境检查主要是了解系统的运行环境是否采取了相关安全措施，涉及对象为网络设备、安全设备、操作系统、数据库、中间件等。在内容上，安全计算环境层面测评实施过程涉及的工作单元，具体如下表：

表4应用系统安全测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 身份鉴别 | 检查所有设备的登录用户是否有身份鉴别措施，是否有复杂度、唯一性等检查。 |
| 2 | 访问控制 | 检查用户的权限分配情况，默认用户和默认口令使用情况等。 |
| 3 | 安全审计 | 检查是否开启安全审计功能，是否能审计到每个用户，审计记录是否有保护措施。 |
| 4 | 入侵防范 | 检查设备在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。 |
| 5 | 恶意代码防范 | 检查设备的恶意代码防范情况。 |
| 6 | 可信验证 | 检查设备是否进行可信验证。 |
| 7 | 数据完整性 | 检查系统数据的传输完整性和存储完整性措施。 |
| 8 | 数据保密性 | 检查系统数据的传输保密性和存储保密性措施。 |
| 9 | 数据备份恢复 | 检查系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。 |
| 10 | 剩余信息保护 | 检查系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。 |
| 11 | 个人信息保护 | 检查系统对个人信息的采集和使用情况。 |

5.3.5安全管理中心

安全管理中心检查主要是了解系统在管理、审计等集中管理的情况，涉及对象为综合管理类设备、综合审计类设备等。在内容上，安全管理中心实施过程涉及的工作单元，具体如下表：

表5安全管理中心测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 系统管理 | 检查是否对系统管理员进行统一的身份鉴别，操作审计等。 |
| 2 | 审计管理 | 检查是否对审计管理员进行统一的身份鉴别，操作审计等。 |
| 3 | 安全管理 | 检查是否对安全管理员进行统一的身份鉴别，操作审计等。 |
| 4 | 集中管控 | 检查是否划分独立的安全管理区域，是否对网络中运行的设备进行状态监测、日志审计、安全审计等，是否对补丁、恶意代代码进行统一管理。 |

5.3.6安全管理制度

安全管理制度测评是为了了解评测安全管理制度的制定、发布、评审和修订等情况，主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及的工作单元，具体如下表：

表6安全管理制度测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 安全策略 | 核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目 标、范围、原则和各类安全策略 |
| 2 | 管理制度 | 检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。 |
| 3 | 制定和发布 | 检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。 |
| 4 | 评审和修订 | 检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。 |

5.3.7安全管理机构

安全管理机构测评是为了了解评测安全管理机构的组成情况和机构工作组织情况，主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。在内容上，安全管理机构测评实施过程涉及的工作单元，具体如下表：

表7安全管理机构测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 岗位设置 | 检查部门/岗位职责文件，测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。 |
| 2 | 人员配备 | 检查人员名单等文档，测评信息系统各个岗位人员配备情况。 |
| 3 | 授权和审批 | 检查相关文档，测评信息系统对关键活动的授权和审批情况。 |
| 4 | 沟通和合作 | 检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。 |
| 5 | 审核和检查 | 检查记录文档等过程，测评信息系统安全工作的审核和检查情况。 |

5.3.8人员安全管理

安全管理人员测评是为了了解单位人员安全方面的情况，主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。在内容上，安全管理人员测评实施过程涉及的工作单元，具体如下表：

表8安全管理人员测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 人员录用 | 检查人员录用文档等过程，测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续办理。 |
| 3 | 安全意识教育和培训 | 检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。 |
| 4 | 外部人员访问管理 | 检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。 |

5.3.9安全建设管理

安全建设管理测评是为了了解评测系统建设管理过程中的安全控制情况，主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全建设管理测评实施过程涉及的工作单元，具体如下表：

表9安全建设管理测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 定级和备案 | 检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。 |
| 2 | 安全方案设计 | 检查系统安全建设方案等文档，测评系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购和使用 | 测评是否按照一定的要求进行系统的产品采购。 |
| 4 | 自行软件开发 | 检查相关软件开发文档等，测评自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 检查相关文档，测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。 |
| 6 | 工程实施 | 检查相关文档，测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 等级测评 | 检查系统之前等级测评的情况，以及之前测评机构的资质等。 |
| 10 | 服务供应商选择 | 测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

5.3.10、安全运维管理

安全运维管理测评是为了了解系统运维管理过程中的安全控制情况，主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，安全运维管理测评实施过程涉及的工作单元，具体如下表：

表10安全运维管理测评内容

|  |  |  |
| --- | --- | --- |
| **序号** | **工作单元名称** | **工作单元描述** |
| 1 | 环境管理 | 检查机房安全管理制度，机房和办公环境等过程，测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 检查资产清单，检查系统、网络设备等过程，测评是否采取必要的措施对系统的资产进行分类标识管理。 |
| 3 | 介质管理 | 检查介质管理记录和各类介质等过程，测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备维护管理 | 检查设备使用管理文档和设备操作规程等过程，测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 漏洞和风险管理 | 检查系统对于漏洞和安全隐患风险的管理，是否有报告、记录等文档，是否定期开展安全测评等。 |
| 6 | 网络和系统安全管理 | 检查系统和网络的安全管理文档，是否明确了角色划分、权限划分，是否覆盖安全策略、账户管理、配置文件的生成及备份、变更审批等内容；检查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修 改等内容；核查是否具有对日志、监测和报警数据等进行分析统计的报告；核查开通远程运维的审批记录，核查针对远程运维的审计日志是否不可以更改等。 |
| 7 | 恶意代码防范管理 | 检查恶意代码防范管理文档和恶意代码检测记录等过程，测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。 |
| 8 | 配置管理 | 检查是否对基本配置信息进行记录和保存，基本配置信息改变后是否及时更新基本配置信息库等。 |
| 9 | 密码管理 | 测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 检查变更方案和变更管理制度等过程，测评是否采取必要的措施对系统发生的变更进行有效管理。 |
| 11 | 备份与恢复管理 | 检查系统备份管理文档和记录等过程，测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。 |
| 12 | 资产管理 | 检查是否有资产清单，清单是否包括资产类别、资产责任部门、 重要程度和所处位置等内容；是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施 的选取上是否不同；核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求。 |
| 13 | 应急预案管理 | 检查应急响应预案文档等过程，测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |
| 14 | 外包运维管理 | 检查外包运维服务情况，单位是否符合国家有关规定，协议是否明确约定外包运维的范围和工作内容等。 |

4.4交付产物

包括但不仅限于以下资料：

|  |  |
| --- | --- |
| 1 | 《网络安全等级保护测评报告》（包含整改建议） |
| 2 | 其他未列入的应交资料 |

注：参与单位应提供书面材料；当发生招标文件目录以外的物资时，以实际发生时间的市场价格为准，供应商不得无故拒绝。

五、提供真实齐全的资质证明文件一份（保证所提供的各种材料和证明材料的真实性，承担相应的法律责任，并请按照下面的顺序装订）：

1.封面（注明包号、品目、公司名称、联系人、联系电话、加盖公司印章）

2.营业执照（副本）营业执照范围须具有信息设备及信息耗材相关资质

3.税务证（国、地税副本）

4.组织机构代码证（副本）

5.经办人授权委托书（原件，见附件1）,法人、经办人身份证复印件。

6.报价一览表（见附件1）

7.特殊条件证明材料：《网络安全等级测评与检测评估机构服务认证证书》。

8.售后服务承诺书（含质量、货源保证，产品验收标准、质保期、售后服务响应等）。

9.其他要求文件。

10.封底

六、报价要求

1.以人民币报价。（报价格式见附件1）

2.报价表中的价格应包括货物设计、材料、制造、包装、运输、装卸、保险、关税、增值税、仓储、商检、卫检、报关、输机、清关手续费、调试、培训、质检、保修、其它伴随服务等所有费用。

3.可提供多种备选产品，分别报价，并分别说明性能、配置及参数。

七、评审方法：

综合评分法（附件2）。

八、其他说明：

1.根据要求及自身实际，用A4纸编制，严格按上述第五条的装订顺序编制资料，并密封。

2.如有，提供相关的产品技术资料。

3.提供的所有资料须加盖鲜章。

4.特别申明：现公示的功能需求、配置及技术性能因市场了解的局限性，仅作为医院参考使用，无任何针对性，如有不全之处，敬请理解，并请参与单位详实介绍推荐产品，最终配置和技术参数以购买时为准。对未公示配置及技术性能的，请各竞选人自行提供。

九、文件递交时间、地点

递交文件截止时间：2022年4月25日17：00前。

递交文件地点：成都市金牛区妇幼保健院8楼院务部。文件必须在递交文件截止时间前送达地点。逾期送达、密封和标注错误的文件，恕不接收。本次采购不接收邮寄的响应文件。

十、其他说明

1.项目解释权归院务部，联系人：张老师68938000。

2.各参会供应商如对此项目有质疑、投诉，请于采购时间截止前即2022年4月25日15：00点前以书面形式向纪检监察室提出，超期不予受理。纪检监察室联系人：邹老师69517102。

附件1

报价表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品  名称 | 品牌 | 型号  参数 | 单位 | 单价（元） | 备注 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**注：**

1.报价应是最终用户验收合格后的总价，包括设备运输、保险、代理、安装调试、培训、税费、系统集成费用和采购文件规定的其它费用。

2.“品目及报价表”为多页的，每页均需由法定代表人或授权代表签字并盖投标人印章。

3.如有多种规格，请按每种规格分别报价。

供应商名称：（盖章）

法定代表人或授权代表（签字）：

日期：

**质量保证书**

：

（制造商家名称）是在 .（国名）依法登记注册的，其地址现在 。其主要营业地点现在 。

作为供应商，我方承诺，为本次招标提供的货物为原厂制造、合法渠道供应的全新产品。我方保证以投标合作者来约束自己，并对该投标共同承担和分别承担招标文件中所规定的义务。

供应商单位名称： （盖章）

供应商单位法定代表人或授权代表（签字）：

日期：

附：授权销售产品清单

**法定代表人身份授权书**

（采购单位名称）：

本授权声明： （投标人名称） （法定代表人姓名、职务）授权 （被授权人姓名、职务）为我方 “ ”项目投标活动的合法代表，以我方名义全权处理该项目有关投标、签订合同以及执行合同等一切事宜。

特此声明。

法定代表人签字：

授权代表签字：

投标人名称： （加盖公章）

日期：

★说明：上述证明文件附有法定代表人、被授权代表身份证复印件（加盖公章）时才能生效。

附件2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素  及权重 | 分　值 | 评分标准 | 说 明 |
| 1 | 报价10% | 10分 | 以满足文件要求且平均报价为基准价，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：报价得分=(基准价／报价)×分值； | 共同评分因素 |
| 2 | 测评方案15% | 测评方案15分 | 根据测评对象、要求和内容制定测评方案，包括①测评流程②测评方法③测评指标④测评进度计划⑤配合需求，共五项。阐述缺项的，每缺一项扣2分；若每项阐述不详尽或存在缺陷的，每项扣1分；未提供测评方案的不得分。 | 共同评分因素 |
| 3 | 实施团队36% | 技术负责人12分 | 拟派技术负责人1名，具有   1. 信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书； 2. 信息安全测评师； 3. 注册信息安全专业人员（CISP）证书； 4. 网络与信息安全应急人员（管理I级）； 5. 具有市级以上职称改革工作领导小组颁发的高级职称证书； 6. 注册云安全系统认证专家（CCSSP）证书。   全部提供得12分，每有一项不提供扣2分，扣完为止。 | 共同评分因素  说明：供应商需提供以上人员证书复印件并加盖供应商公章。 |
| 项目经理  14分 | 拟派项目经理1名，具有   1. 信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书； 2. 信息安全测评师； 3. 网络与信息安全应急人员（管理I级）； 4. 注册云安全系统认证专家（CCSSP）证书； 5. 信息安全保障人员（CISAW）（认证方向：应急服务）； 6. 计算机软件产品检验员证书; 7. 获得过国家信息安全等级保护工作协调小组办公室颁发的个人荣誉证书。全部提供得14分，每有一项不提供扣2分，扣完为止。 | 共同评分因素  说明：供应商需提供以上人员证书复印件并加盖供应商公章。 |
| 测试人员10分 | 测试人员2名，具有   1. 网络与信息安全应急人员（技术I级）; 2. 注册网络安全专业防御人员（NSATP-D）; 3. 信息安全保障人员（CISAW）； 4. 注册云安全系统认证专家（CCSSP）证书； 5. 计算机技术与软件专业技术资格（信息安全工程师）证书。   每提供一人含上述任意证书的得2分，同一证书不重复得分，最高得10分，不提供不得分。 | 共同评分因素  说明：供应商需提供以上人员证书复印件并加盖供应商公章。 |
| 6 | 供应商业绩10% | 10分 | 2019年1月1日至投标截止日起，每具有1个类似项目业绩得2分，最多得10分。 | 共同评分因素  说明：供应商需提供合同复印件或中标（成交）通知书复印件并加盖供应商单位公章。 |
| 7 | 企业资质29% | 29分 | 1.具有ISO9001质量管理体系认证证书, 认证范围包括“评估测试服务”得3分；  2.具有ISO20000信息技术服务管理体系证书, 认证范围包括“评估测试服务”得3分；  3.具有ISO27001信息安全管理体系证书, 认证范围包括“评估测试服务”得3分；  4.投标人具有工业信息安全应急服务支撑单位证书得3分；  5.具有工业信息安全测试评估机构能力认定证书得3分；  6.供应商具有中国合格评定国家认可委员会颁发的检验机构认可证书（CNAS），认可检验能力范围涵盖“信息系统网络安全等级保护测评”的得4分；  7.投标人在2018年至今，具有一份及以上CNVD颁发的“原创漏洞证明”证书，一个得1分，最高得10分。 | 共同评分因素  说明：供应商需提供有效证明文件复印件并加盖供应商公章。 |