磋 商 文 件

（服务类）

采购项目名称：网络安全等级保护项目及网络安全等级保护测评项目

采购项目编号：**N5107032023000202**

绵阳市肿瘤医院

绵阳正信工程造价咨询有限公司共同编制

2023年**12**月**18**日

第一章 竞争性磋商邀请

绵阳正信工程造价咨询有限公司（以下简称“代理机构”）受绵阳市肿瘤医院委托，拟对网络安全等级保护项目及网络安全等级保护测评项目采用竞争性磋商采购方式进行采购，兹邀请供应商参加本项目的竞争性磋商。

一、项目编号：N5107032023000202

二、项目名称：网络安全等级保护项目及网络安全等级保护测评项目

三、磋商项目简介

绵阳正信工程造价咨询有限公司受绵阳市肿瘤医院委托，拟对网络安全等级保护项目及网络安全等级保护测评项目采用竞争性磋商采购方式进行采购，兹邀请供应商参加本项目的竞争性磋商。

四、邀请供应商

本次采购采取公告征集邀请磋商的供应商。

公告征集：本次竞争性磋商在“四川政府采购网（www.ccgp-sichuan.gov.cn）”上以公告形式发布，兹邀请符合本次采购要求的供应商参加本项目的竞争性磋商。

五、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

执行政府采购促进中小企业发展的相关政策：

采购包1（网络安全等级保护项目）：属于专门面向中小企业采购。

采购包2（网络安全等级保护测评）：属于专门面向中小企业采购。

注：监狱企业和残疾人福利性单位视同小微企业，符合中小企业划分标准的个体工商户视同中小企业。

（三）本项目的特定资格要求：

采购包1：

1、参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。（描述：参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。）

采购包2：

1、参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。（描述：参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。）

2、具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》（描述：具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》）

六、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：四川省政府采购一体化平台（以下简称“采购一体化平台”）的项目电子化交易系统（以下简称项目电子化交易系统），登录方式及地址：通过四川政府采购网（www.ccgp-sichuan.gov.cn）首页供应商用户登录采购一体化平台，进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在四川政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用采购一体化平台前，应当按照要求完成供应商注册和信息完善，加入采购一体化平台供应商库。

（二）供应商应当使用纳入全国公共资源交易平台（四川省）数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录采购一体化平台进行的一切操作和资料传递，以及加盖电子签

章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看四川政府采购网-办事指南。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）采购一体化平台技术支持：

在线客服：通过四川政府采购网-在线客服进行咨询

400服务电话：4001600900

CA及签章服务：通过四川政府采购网-办事指南进行查询

七、竞争性磋商文件获取时间、方式及地址

（一）磋商文件获取时间：详见采购公告或邀请书。

（二）在磋商文件获取开始时间前，采购人或代理机构将本项目磋商文件上传至项目电子化交易系统，免费向供应商提供。供应商通过项目电子化交易系统获取磋商文件。成功获取磋商文件的，供应商将收到已获取磋商文件的回执函。未成功获取磋商文件的供应商，不得参与本次采购活动，不得对磋商文件提起质疑。

成功获取磋商文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响响应文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的磋商文件，供应商应当重新获取磋商文件。供应商未重新获取磋商文件或者未按照澄清或者修改后的磋商文件编制响应文件进行响应的，自行承担不利后果。

注：获取的磋商文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

八、首次响应文件提交截止时间及开启时间、地点、方式

（一）提交首次响应文件截止时间及开启时间：详见采购公告或邀请书。

（二）响应文件提交方式、地点：供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统提交响应文件。成功提交的，供应商将收到已提交响应文件的回执函。

九、磋商方式

本项目磋商小组与供应商通过项目电子化交易系统以在线方式进行磋商。磋商会议由磋商小组在线主持，供应商代表在线参加。供应商应随时关注项目电子化交易系统信息，及时参与在线磋商。供应商登录项目电子化交易系统，与磋商小组进行在线磋商、提交供应商响应表，供应商响应表应加盖供应商（法定名称）电子印章。

十、供应商信用融资

根据《四川省财政厅关于推进四川省政府采购供应商信用融资工作的通知》（川财采〔2018〕123号）文件，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录四川政府采购网—金融服务平台，选择符合自身情况的“政采贷”银行及其产品，凭项目成交结果、成交通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

十一、联系方式

采购人： 绵阳市肿瘤医院

地址： 绵阳市涪城区长虹大道107号

邮编： 621000

联系人： 何彬艳

联系电话： 15984656127

代理机构：绵阳正信工程造价咨询有限公司

地址： 四川省绵阳市涪城区安昌路17号富临花园四楼15号

邮编： 621000

联系人： 何帆

联系电话： 18181761229

第二章 供应商须知

2.1供应商须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	本项目各包采购预算金额如下： 采购包1：170,000.00元 采购包2：240,000.00元 供应商采购包报价高于采购包采购预算的，其响应文件将按无效处理。
2	最高限价（实质性要求）	详见第三章。 供应商的采购包响应报价高于最高限价的，其响应文件将按无效处理。
3	评审方法	综合评分法(详见第五章)。
4	是否接受联合体	采购包1：不接受联合体 采购包2：不接受联合体
5	落实节能、环保、无线局域网	1.根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。 2.本项目采购的 无 产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效响应处理。 3.本项目采购的 无 产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购的 无 产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。 4.响应产品属于中国政府采购网公布的《无线局域网认证产品政府采购清单》且在有效期内的，按《财政部 国家发展改革委 信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号）要求优先采购。
6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）的规定， 关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第五章。

7	充分、公平竞争保障措施（实质性要求）	核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。 提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下采购活动的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交供应商推荐资格；最后评审得分相同的，由采购人或者采购人委托磋商小组采取随机抽取方式确定一个供应商获得成交供应商推荐资格，其他同品牌供应商不作为成交候选人。 核心产品清单详见第三章。 在符合性审查、有效报价环节提供核心产品品牌不足3个的，视为有效响应供应商不足3家。
8	不正当竞争预防措施（实质性要求）	在磋商过程中，磋商小组认为供应商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，磋商小组应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。供应商提交的书面说明，应当加盖供应商公章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其响应报价合理性。供应商不能证明其响应报价合理性的，磋商小组应当将其响应文件作为无效处理。（注：供应商报价低于最高限价50%或者低于其他有效供应商报价算术平均价40%的，磋商小组可以认为该供应商“报价明显低于其他实质性响应的供应商报价”。）
9	磋商保证金	本项目不收取磋商保证金。
10	履约保证金（实质性要求）	采购包1：不收取 采购包2：不收取
11	响应有效期（实质性要求）	提交首次响应文件的截止之日起不少于90天。
12	招标代理服务费（实质性要求）	本项目收取代理服务费 代理服务费用收取对象：中标/成交供应商 代理服务费收费标准：按照“成本+合理利润”原则，由成交人向采购代理机构支付。
13	采购结果公告	采购结果将在四川政府采购网予以公告。
14	成交通知书	采购结果公告后，采购人或代理机构通过项目电子化交易系统向成交供应商发出成交通知书；成交供应商通过项目电子化交易系统获取成交通知书。
15	政府采购合同公告、备案	政府采购合同签订之日起2个工作日内，采购人将政府采购合同在四川政府采购网予以公告；政府采购合同签订之日起7个工作日内，采购人将政府采购合同报本级财政部门备案。
16	进口产品	不允许（实质性要求）
17	是否组织潜在供应商现场考察	采购包1：否 采购包2：否
18	特殊情况	出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法终止采购活动。

19	报价/分值精确度	报价/分值精确度仅保留“所有数据项默认最多可输入/展示至小数点后2位，超出小数点位的数值采用四舍五入的方式进行精确。”

2.2总则

2.2.1适用范围

一、本磋商文件仅适用于本次竞争性磋商采购项目。

二、本磋商文件的最终解释权由绵阳市肿瘤医院和绵阳正信工程造价咨询有限公司享有。对磋商文件中供应商参加本次政府采购活动应当具备的条件，磋商项目技术、服务、商务及其他要求，评审细则及标准由绵阳市肿瘤医院负责解释。除上述磋商文件内容，其他内容由绵阳正信工程造价咨询有限公司负责解释。

2.2.2有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次磋商的采购人是绵阳市肿瘤医院。

二、“供应商”是指在按照磋商公告规定获取磋商文件，拟参加响应和向采购人提供货物及相应服务的法人、其他组织或自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是绵阳正信工程造价咨询有限公司。

四、“网上开启”是指供应商通过项目电子化交易系统在线完成签到、响应文件解密后，采购人或者采购代理机构通过项目电子化交易系统在线完成已解密响应文件的开启工作。

五、“电子评审”是指通过项目电子化交易系统在线完成磋商小组组建，开展资格和符合性审查、比较与评价、出具磋商报告、推荐成交候选供应商等活动。

2.2.3响应费用（实质性要求）

供应商应自行承担参加竞争性磋商采购活动的全部费用。

2.3磋商文件

2.3.1磋商文件的构成

一、磋商文件是供应商准备响应文件和参加响应的依据，同时也是评审的重要依据。磋商文件用以阐明磋商项目所需的资质、技术、服务及报价等要求、磋商程序、有关规定和注意事项以及合同草案条款等。本磋商文件包括以下内容：

（一）竞争性磋商邀请；

（二）供应商须知；

（三）磋商项目技术、服务、商务及其他要求；

（四）磋商过程中可实质性变动的内容；

（五）磋商办法；

（六）响应文件格式；

（七）拟签订采购合同文本。

二、供应商应认真阅读和充分理解磋商文件中所有的事项、格式条款和规范要求。供应商没有对磋商文件全面作出实质性响应所产生的风险由供应商承担。

2.3.2磋商文件的澄清和修改

一、在提交首次响应文件截止时间前，采购人或者代理机构可以对已发出的磋商文件进行必要的澄清或者修改。

二、澄清或者修改的内容为磋商文件的组成部分，采购人或者代理机构将在四川政府采购网发布更正公告，供应商应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响响应文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的磋商文件，供应商应依据更正后的磋商文件编制响应文件。若供应商未按前述要求进行响应的，自行承担不利后果。

2.4响应文件

2.4.1响应文件的语言

一、供应商提交的响应文件以及供应商与磋商小组在磋商过程中的所有来往书面文件均须使用中文。响应文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，磋商小组将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对供应商的不利后果，由供应商承担。

2.4.2计量单位（实质性要求）

除磋商文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3响应货币（实质性要求）

本次项目均以人民币报价。

2.4.4知识产权（实质性要求）

一、供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如存在前述情形，由供应商承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、供应商将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用供应商所不拥有的知识产权，则在报价中必须包括合法使用该知识产权的相关费用。

2.4.5响应文件的组成（实质性要求）

供应商应按照磋商文件的规定和要求编制响应文件。

响应文件具体内容详见第六章。

2.4.6响应文件格式

一、供应商应按照磋商文件第六章中提供的“响应文件格式”填写相关内容。

二、对于没有格式要求的响应文件由供应商自行编写。

2.4.7响应报价（实质性要求）

一、供应商的报价是供应商响应磋商项目要求的全部工作内容的价格体现，包括供应商完成本项目所需的一切费用。

二、响应文件报价出现前后不一致的，按照磋商文件第五章磋商办法规定予以修正，修正后的报价经供应商以书面形式通过项目电子化交易系统进行确认，并加盖供应商（法定名称）电子印章，供应商逾时确认的，其响应无效。

2.4.8响应有效期（实质性要求）

响应有效期详见第二章“供应商须知前附表”，响应文件未明确响应有效期或者响应有效期小于“供应商须知前附表”中响应有效期要求的，其响应文件按无效处理。

2.4.9响应文件的制作、签章和加密

一、响应文件应当根据磋商文件进行编制。供应商应通过四川政府采购网-办事指南下载响应客户端，使用客户端编制响应文件。

二、供应商应按照客户端操作要求，对应磋商文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合磋商文件对应项的要求的，其响应文件作无效处理。

三、供应商完成响应文件编制后，应按照响应文件第一章明确的签章要求，使用互认的证书及签章对响应文件进行电子签章和加密。

四、磋商文件澄清或者修改的内容可能影响响应文件编制的，代理机构将重新发布澄清或者修改后的磋商文件，供应商应重新获取澄清或者修改后的磋商文件，按照澄清或者修改后的磋商文件进行响应文件编制、签章和加密。

2.4.10响应文件的提交（实质性要求）

一、供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统完成响应文件提交。

二、在提交首次响应文件截止时间后，代理机构不再接受供应商提交响应文件。供应商应充分考虑影响响应文件提交的各种因素，确保在提交首次响应文件截止时间前完成提交。

2.4.11响应文件的补充、修改（实质性要求）

响应文件提交截止时间前，供应商可以补充、修改或者撤回已成功提交的响应文件；对响应文件进行补充、修改的，应当先行撤回已提交的响应文件，补充、修改后重新提交。

供应商响应文件撤回后，视为未提交过响应文件。

2.5开启、资格审查、磋商和确定成交供应商

2.5.1磋商开启程序

一、本项目为竞争性磋商项目。网上开启的开始时间为响应文件提交截止时间。成功提交或成功提交和解密电子响应文件的供应商不足3家的，不予开启，采购人或代理机构将终止采购活动。

二、磋商开启准备工作

响应文件开启时间前，供应商登录项目电子化交易系统-“开标/开启大厅”，等待代理机构开启磋商。

三、解密响应文件（实质性要求）

响应文件提交截止时间后，成功提交响应文件的供应商符合响应文件规定数量的，代理机构将启动响应文件解密程序，解密时间为30分钟；供应商应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行响应文件解密。供应商未在规定的解密时间内完成解密的，按无效响应处理。

开启过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。供应商对开启过程和开启记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对供应商提出的询问或者回避申请应当及时处理。

2.5.2查询及使用信用记录

开启结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询供应商在响应文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3资格审查

详见磋商文件第五章。

2.5.4磋商

详见磋商文件第五章。

2.5.5成交通知书

一、采购人或者磋商小组确认成交供应商后，代理机构在四川政府采购网发布成交结果公告、通过项目电子化交易系统发出成交通知书，成交供应商通过项目电子化交易系统获取成交通知书。

二、成交通知书是采购人和成交供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的成交无效情形的，将以公告形式宣布发出的成交通知书无效，成交通知书将自动失效，并依法重新确定成交供应商或者重新开展采购活动。

三、成交通知书对采购人和成交供应商均具有法律效力。

2.6签订及履行合同和验收

2.6.1签订合同

一、采购人应在成交通知书发出之日起三十日内与成交供应商签订采购合同。

二、采购人和成交供应商签订的采购合同不得对磋商文件确定的事项以及成交供应商的响应文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于成交供应商的主要合同义务。

三、采购合同实行分包履行的，成交供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包；

采购包2：不允许合同分包；

2.6.2.2合同转包

一、严禁成交供应商将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、成交供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，在不改变合同其他条款的前提下，可以与成交供应商协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2.6.4履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

2.6.5履约验收方案

采购包1：

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起10日内组织验收

8）验收组织的其他事项：签订合同时约定

9）技术履约验收内容：签订合同时约定

10）商务履约验收内容：签订合同时约定

11）履约验收标准：

中标人与采购人应严格按照按国家有关规定、采购文件的服务要求、成交供应商响应文件及承诺以及合同约定标准及根据《政府采购需求管理办法》（财库〔2021〕22号）文件的规定，同时参照《四川省政府采购项目需求论证和履约验收管理办法》（财库〔2016〕205号）文件的要求及国家行业主管部门规定的标准、方法和内容组织验收。

12）履约验收其他事项：无

采购包2：

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请服务对象：否

5）是否邀请第三方检测机构：否

6）履约验收程序：一次性验收

7）履约验收时间：

供应商提出验收申请之日起10日内组织验收

8）验收组织的其他事项：签订合同时约定

9）技术履约验收内容：签订合同时约定

10）商务履约验收内容：签订合同时约定

11）履约验收标准：

中标人与采购人应严格按照按国家有关规定、采购文件的服务要求、成交供应商响应文件及承诺以及合同约定标准及根据《政府采购需求管理办法》（财库〔2021〕22号）文件的规定，同时参照《四川省政府采购项目需求论证和履约验收管理办法》（财库〔2016〕205号）文件的要求及国家行业主管部门规定的标准、方法和内容组织验收。

12）履约验收其他事项：签订合同时约定

2.6.6资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7响应纪律要求

2.7.1磋商活动纪律要求

采购人、代理机构应保证磋商活动在严格保密的情况下进行，采购人、代理机构、供应商和磋商小组成员应当严格遵守政府采购法律法规规章制度和本项目磋商文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响磋商过程和结果。

对各供应商的商业秘密，磋商小组成员应予以保密，不得泄露给其他供应商。

2.7.2供应商不得具有的情形（实质性要求）

供应商参加响应不得有下列情形：

一、有下列情形之一的，视为供应商串通响应：

（一）不同供应商的响应文件由同一单位或者个人编制；

（二）不同供应商委托同一单位或者个人办理磋商事宜；

（三）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

（四）不同供应商的响应文件异常一致或者响应报价呈规律性差异；

（五）不同供应商的响应文件相互混装。

二、提供虚假材料谋取成交；

三、采取不正当手段诋毁、排挤其他供应商；

四、与采购人或代理机构、其他供应商恶意串通；

五、向采购人或代理机构、磋商小组成员行贿或者提供其他不正当利益；

六、在磋商过程中与采购人或代理机构进行协商磋商；

七、成交后无正当理由拒不与采购人签订政府采购合同；

八、未按照磋商文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

供应商有上述情形的，按照规定追究法律责任，具有前述一至十一条情形之一的，其响应文件无效，或取消被确认为成交供应商的资格或认定成交无效。

2.7.3采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与供应商有下列利害关系之一的，应当回避：

（一）参加采购活动前3年内与供应商存在劳动关系；

（二）参加采购活动前3年内担任供应商的董事、监事；

（三）参加采购活动前3年内是供应商的控股股东或者实际控制人；

（四）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

（五）与供应商有其他可能影响政府采购活动公平、公正进行的关系。

供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

2.8询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对采购文件中采购需求的询问、质疑由 绵阳正信工程造价咨询有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由绵阳正信工程造价咨询有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 绵阳正信工程造价咨询有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处理解决（包含但不限于文字错误、标点符号、不影响响应文件的编制的情形）。

四、供应商认为磋商文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；

（二）对采购过程提出质疑的，为各采购程序环节结束之日；

（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料：

（一）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）

（二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；

（三）法定代表人或主要负责人身份证复印件1份；

（四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；

（五）针对质疑事项必要的证明材料（针对磋商文件提出的质疑，需提交从项目电子化交易系统获取的磋商文件回执单）。

答复主体：代理机构

联系人：欧阳青强

联系电话：15681231025

地址：绵阳市涪城区安昌路17号富临花园4楼15号

邮编：621000

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出磋商文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1、采购项目概况

网络安全等级保护项目及网络安全等级保护测评项目

3.2、服务内容及服务要求

3.2.1服务内容

采购包1：

采购包预算金额（元）：170,000.00

采购包最高限价（元）：170,000.00

序号	标的名称	数量	标的金额 （元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	网络安全等级保护	1.00	170,000.00	项	其他未列明行业	否	否	否	否

采购包2：

采购包预算金额（元）：240,000.00

采购包最高限价（元）：240,000.00

序号	标的名称	数量	标的金额 （元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	网络安全等级保护测评	1.00	240,000.00	项	其他未列明行业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：网络安全等级保护

参数性质	序号	技术参数与性能指标
		项目要求 序号 | 采购内容 | 技术描述 | 单位 | 数量

		1	绿盟防火墙一年设备续保	★1、用于防火墙特征库实时升级和硬件维保，防止来自被保护区域外部的攻击。在需要被保护的网络边界上设置防火墙，可以保护易受攻击的网络服务资源。	套	1
		2	绿盟入侵防御一年设备续保	★1、用于入侵防御特征库实时升级和硬件维保，能够在检测到入侵时，实时对入侵活动和攻击性网络流量进行拦截，将对网络的入侵降到最低	套	1
		3	绿盟堡垒机一年设备续保	★1、用于堡垒授权升级和硬件维保，堡经机主账号通过本地认证、3A认证、RADIUS认证等多种认证方式，将主账号与实际运维用户身份一一对应，确保行为审计的一致性，以而准确定位事故责任人，弥补传统网络安全审计产品无法准确定位运维用户身份的缺陷。	套	1
		4	绿盟日志审计一年设备续保	★1、用于日志审计授权升级和硬件维保，用于记录用户操作的审计日志，快速定位问题的根源。追踪程序执行的过程。追踪数据的变化，数据统计和性能分析，采集运行环境数据	套	1
				★1、提供 350个终端点位授权（340个Windows版本、10个LINUX版本，服务器和桌面终端共用）。授权包含终端管理后台以及全模块功能（反病毒引擎、多层次主动防御系统、病毒防御、系统防御、网络防御、设备控制等），无需按照模块进行授权。 ★2、提供三年病毒库更新升级服务。 ★3、非OEM产品，厂商具备自主研发反病毒引擎、行为沙盒分析模块、病毒实时监控模块等能力。 ★4、所提供产品为保护用户的隐私权、数据所有权，不会上传用户的任何文件、数据等信息，仅在用户中心控制台联网升级的情况下，上传用户许可相关信息（License），用于验证正版授权。 5、支持采用B/S架构，由控制中心、系统中心、客户端三个模块组成防病毒体系，管理员只需通过浏览器登录控制中心，即可对系统进行管理。 ▲6、控制中心和客户端均支持Windows XP、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows Server 2003、W		

				indows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019。客户端支持CentOS、Ubuntu、SUSE、Deepin、凝思等主流Linux发行操作系统以及中标麒麟、银河麒麟、红旗、统信、等国产操作系统，一个控制中心能够管控所有支持终端。 ▲7、要求中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将自动顶替宕机的主中心且同步数据（提供证明资料并加盖投标人公章）。 8、要求中心配备安全工具及管理工具：域部署工具、离线升级工具、中心迁移工具、移动存储注册工具、专杀工具。 9、要求中心可对全网终端下发登记任务，需登记的信息可自定义内容，支持设置必填项或非必填项；且可开启终端安装资产登记功能，运行安装包后需先填写登记信息才可继续安装。 10、客户端部署支持本地部署、网页访问部署、域推送安装方式。 11、控制中心支持直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。 12、要求展示终端基本信息：终端名称、计算机名称、本地IP、通信IP、MAC地址、终端类型、操作系统版本、病毒库版本、终端版本、唯一标识、防御功能状态、禁网状态、策略同步状态、最近登录用户、上线时间、终端标签等。能组合检索项进行全方位查询、定位、展示。 13、要求支持基于HTTP协议的数据流量检测，可检测恶意代码并追溯恶意代码来源 ▲14、要求支持中心二次验证，开启该功能后，通过登录中心时进行二次验证的方式，阻止中心遭遇密码泄露、弱口令暴破、撞库等黑客破解行为带来的危害，达到保护控制中心的目的。 15、支持客户端主动升级及平台即时/定时推送升级；平台支持客户端升级包上传及配置http(s)/ftp远端同步方式，更新客户端升级包，可以根据不同网络环境提供在线获取和隔离网获取相		

		5	杀毒软件	应工具。 16、要求中心支持任务通知，可在任务完成时、硬件变更时、终端安全服务异常时、子中心连入时、子中心脱离时接收通知 ▲17、要求具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出。用户需再次输入正确的动态口令才可登入计算机。且可设置应用范围：远程登录时启用或本地登录时启用（提供证明资料并加盖投标人公章）。 18、支持第三方软件调用API接口，包括调用接口获取全部分组信息、调用接口创建分组、调用接口修改分组名称、调用接口删除分组、调用接口查询上线终端情况、调用接口查询终端详情、调用接口修改终端名称、调用接口修改终端分组、调用接口查询终端详情 ▲19、支持定制策略包括病毒防御（文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP协议控制、IP黑名单）等，可以根据部门需求定制不同的策略（提供证明资料并加盖投标人公章）。 20、支持全局信任区，全局信任区有信任文件路径、信任文件校验和方法，方便添加信任文件。 21、支持统计分析客户端上报的威胁日志，包含终端/部门/责任人危险排行、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等，要求支持管理员操作，日志记录追踪；支持控制中心-客户端交互操作，日志记录追踪，便于问题定位。 ▲22、支持“软件禁用”功能，管理员可按分组设置禁用软件策略；“终端发现”功能，方便管理员查看未安装客户端的终端情况；“违规外联”功能，检测终端是否违规连接外部网络，并进行管控；“时间同步”设置，开启后终端与中心系统时间将保持一致。 23、具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能	点	350	

				力与断网时的病毒查杀能力一致）。具有轻量级的病毒库，却有较强的病毒查杀能力。 ▲24、支持反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本。要求虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力（提供证明资料并加盖投标人公章）。 25、要求支持勒索病毒诱捕，可在根目录生成txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离。 26、要求反病毒引擎具有基于虚拟沙盒的动态行为分析，可以跟踪和记录运行在其中程序的行为，通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估。 ▲27、要求中心具有远程桌面功能，可关闭系统自带的远程桌面，使用自研远程桌面功能替代，预防黑客远程桌面爆破。 ▲28、支持windows客户端防护具有系统加固功能，阻止某些流氓、广告程序对电脑系统的恶意篡改等行为，提供一套全方位的加固方案，保护电脑系统各个安全关键点。其中默认开启文件防护≥9项,注册表保护≥26项，敏感动作防护≥29项. ▲29、要求windows客户端防护同时具备桌面右下角广告弹窗拦截具有桌面右下角广告弹窗拦截和软件安装拦截功能，安装软件的时候帮助用户识别软件是否是推广软件，用户可以自由选择是否需要继续安装；当有发现有推广软件正在安装时，会弹窗提示， 用户可以根据需要选择是否安装此软件。 ▲30、要求具有黑客入侵拦截功能，检测通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免电脑遭到黑客入侵。直接从网络层防御Wanncry、MS 08-067等漏洞攻击。 31、要求支持暴破攻击防护，阻止黑客通过SMBv1、SMBv2、 RPC、SQLServer、PDP协议进行暴力破解攻击 ▲32、要求支持无需沙箱即可针对包括但不限			

	1			于Web服务器、数据库软件、Office软件、编辑软件、浏览器、设计软件等软件进行加固，防止前述软件漏洞被攻击者（人或程序）利用进而进行渗透攻击。 33、要求具有设备控制功能，可管控U盘、便携设备、USB无线网卡、USB有限网卡、打印机、光驱、蓝牙设备。 ▲34、开启U盘禁用后，客户端可远程申请使用U盘，管理员可根据实际应用场景临时开放U盘使用权限。 35、要求具有U盘信任功能，当终端开启访问控制-设备控制-U盘设备时，可以通过在中心的“信任设备”功能来添加需要信任的移动存储设备，以允许该设备在任意终端使用。 ▲36、要求支持对U盘注册的同时进行加密，即使U盘丢失，也可保护数据，防止数据泄露 ▲37、考虑到我院部分电脑配置很低，业务系统众多与稳定运行的重要性，要求投标产品的客户端安装后最多占用60M硬盘空间，最多10M的病毒库大小，日常内存占用不到30M，有效节省电脑资源。实现对终端资源占用影响小，让位于业务系统，且不影响查杀效率（提供证明资料并加盖投标人公章）。 ▲38、为更好的保障本项目实施质量，需提供针对本项目的原厂售后服务承诺函（中标后签订合同前提供承诺函并加盖制造商公章）		
				1、★产品应为国产品牌，提供该系统的计算机软件著作权登记证书和计算机信息系统安全专用产品销售许可证的复印件并加盖投标人公章； 2、▲本次配置文件防御，防勒索，内核加固，应用伪装。为方便后续添加功能模块，产品还应支持微隔离、网络防御、防篡改、风险发现、等安全加固模块。为实现有效联动防御，以上所有模块应为同一品牌、同一后台、统一账号管理并进行综合日志分析；（提供截图并加盖投标人公章）。 3、客户端环境支持主流服务器操作系统，包括Windows Server 2008 R2、Windows Server 2012、Windows Server 2016、Windows Server 2019、RedHat6.0-7.9、CentOS		

				6.0-7.9等系统版本； 4、支持多用户，多角色管理；支持用户分级管理模式，能对不同的用户设置不同的权限、管理不同的资产、不同的子系统授权； 5、支持资产信息的基本管理及统计，能对添加的资产设置属性，如名称、描述、位置、所属部门、责任人、所属业务系统、对应机器、用户组等； 6、符合等保2.0的安全要求：具备三权分离功能，syslog发送功能，传输采用https加密，存储加密，支持登录失败保护等基线要求； 7、支持对客户端所在服务器的操作系统类型与在线情况的统计； 8、支持对访问IP设置白名单，限制对平台的访问时间；（提供截图并加盖投标人公章） ▲9、能对ASP、ASPX、PHP、JSP等常见的网页木马文件进行无限制脱壳解密，Web恶意脚本的查杀识别准确率不低于测试样本总数的95%；有主动防御技术，对于文件的复制、移动、修改、重命名以及下载上传等都能做到监控；拥有文件防篡改功能；有系统账户保护功能，防止操作系统账户被修改或增加；针对该条指标应提供中国合格评定国家认可委员会（CNAS）认可的实验室出具的软件测试报告复印件并加盖投标人公章。 10、日志管理：支持平台日志信息的记录、导出及超时日志的自动清理； 11、支持平台及各子系统数据库的备份与恢复，允许清除备份数据； 12、支持平台信息的图形化统计展示，包括但不限于授权信息、服务器信息（含CPU、内存、硬盘使用率等）、综合概况（资产、主机、系统等数量）、各子系统攻防次数统计（微隔离、网络防御、文件防御、防篡改、防勒索、内核加固）等。 13、内置webshell检测方法及装置；支持按高、中、低敏感度自动处理Web恶意脚本；支持按全盘和自定义目录查杀Web恶意脚本；支持按文件、目录、后缀、进程等类型设置排除策略；支持脚本限制，系统将根据设定的规则（如设置保护目录）对脚本文件创建或修改进行限制		

		6	AI加固软件	支持对处置文件的原样保存及隔离；支持对隔离文件的还原；支持批量操作，如删除资产、设置功能开关、开始或停止查杀、增加/删除/启用/禁用限制策略或排除策略、删除/清空/导出日志等。支持文件防御日志详情展示，包括但不限于文件路径、所属进程、处理结果、攻击时间、攻击描述等；支持文件防御信息的图形化统计展示，包括但不限于主动防御安全趋势（含仅记录、已隔离、疑似类型、危险关系、扫描来源、主动防御来源等文件主动防御信息的年、月、日趋势）等。 ▲14、拥有系统防勒索功能，基于驱动级拦截技术实现针对勒索病毒及恶意代码的防护，不依赖于特征库识别方式防御勒索病毒攻击，开启防御后保护目录只拥有防勒索策略中的权限和可读权限。能自行设定防勒索规则，如：特定进程、特定范围、特定文件、特定格式等。（提供截图并加盖投标人公章）。 15、关键应用保护机制：支持应用白名单信任机制，信任机制至少包括识别进程名、程序签名及安全标签（程序哈希值）三种方式； 数据库文件保护：内置数据库文件保护引擎，防范RootKit攻击，使数据库文件免受勒索病毒或恶意代码的加密、添加、修改和删除，包括但不限于Oracle、MSSql Server、Mysql、DB2、DM、人大金仓、达梦、优炫等所有类型数据库； 16、文档保护：支持自动保护非结构化文档，可根据独立文件名、后缀和目录提供自定义配置； ▲17、堡垒模式：支持对特定终端实现强安全保护模式，禁止任何新应用程序的运行，有效防止包括勒索软件、已知勒索病毒、未知勒索病毒、挖矿病毒等恶意攻击；（提供截图并加盖投标人公章） 18、可禁止未授权的外部移动存储设备接入服务器传播危险程序。 19、可禁止在网络驱动器上执行任何程序，如Windows映射驱动器、Linux服务器挂载的其它磁盘等。 20、支持批量操作，如删除资产、设置功能	点	8	

				开关、增加/删除/启用/禁用防勒索策略、删除/清空/导出日志等。 21、支持防勒索日志详情展示，包括但不限于勒索进程、对应文件、勒索时间等； 22、支持防勒索信息的图形化统计展示，包括但不限于被勒索资产排行、被勒索时间分布概览、防勒索安全趋势（含创建、删除、修改、移动等权限的年、月、日趋势）等。 26、支持对Web服务器进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持IIS、Apache、Nginx等Web服务软件禁止执行某个程序； 支持对数据库进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持MongoDB 命令行进程、MongoDB 共享服务进程、MongoDB 核心进程、Oracle 监听服务进程、Oracle 核心进程、Mysql数据库客户端、Mysql数据库核心进程、Mssql数据库核心进程等禁止执行某个程序； 23、支持对应用运行环境进行加固，依据设定的规则对特定的项进行执行限制，包括但不限于支持Node.js、Java、PHP FastCGI、PHP等运行环境禁止执行某个程序； 24、支持对Windows、Linux服务器其它特定进程进行加固：特定进程将受到限制，具体行为依据设定的规则； 25、允许在应用加固规则中设置白名单，支持设置程序名或全路径等信息。 26、支持批量操作，如删除资产、设置功能开关、增加/启用/禁用规则组策略、删除/清空/导出日志等。 27、支持内核加固日志详情展示，包括但不限于日志类型、程序名或全路径、目标名称、攻击时间等； 28、支持内核加固信息的图形化统计展示，包括但不限于攻击类型统计、受攻击资产排行、攻击规则排行、受攻击时间分布概览、内核加固安全趋势等。 ▲29、拥有应用伪装功能，能根据设定的规则（如端口号、描述、协议等）自动开启端口。允许设置连接次数阈值、数据包数阈值和间隔时间		

				等；（提供截图并加盖投标人公章）能根据对伪装端端口的访问自动判别是否非法访问； 30、支持批量操作，如删除资产、设置功能开关、增加/删除/启用/禁用伪装端口、删除/清空/导出日志等； 31、支持应用伪装日志详情展示，包括但不限于端口号、来源地址、来源类型、描述、攻击时间等； 支持应用伪装信息的图形化统计展示，包括但不限于总类型占比、总资产排行、总时间分布概况、总端口排行、应用伪装趋势（含连接次数、数据包数等信息的年、月、日趋势）等。		

1、本次项目防火墙、入侵防御、堡垒机、日志审计需提供一年设备续保。杀毒软件三年有效授权，AI安全加固一年有效授权，提供原厂售后服务承诺函。

2、投标人需要单独承诺，协助用户达到二级等级保护标准，并取得备案证书，否则由此产生的一切后果由中标人自行承担。

3、中标供应商应积极与采购人沟通协商合同条款，双方协商一致方可签订项目采购服务合同。中标供应商在签订项目采购服务合同之前，采购人有权要求对本项目涉及到的软硬件设备的功能、性能及供应商服务能力进行逐一验证核查，若有任何一项与投标技术应答不符即视为虚假应标，取消其中标资格，并追究中标供应商递交虚假资料的法律责任，同时承担相应损失。

采购包2：

标的名称：网络安全等级保护测评

参数性质	序号	技术参数与性能指标
		（一）项目目标及范围 根据《中华人民共和国网络安全法》、《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，对绵阳市肿瘤医院的信息系统开展等级保护测评服务和信息安全服务工作，同时针对HIS系统、电子病历系统进行渗透测试，开展一次攻防演练，出具演练报告，以及网络安全培训一次，突发网络安全事件10分钟响应，1小时内到达现场进行应急处理。本次服务相关信息系统情况如下：

序号	信息系统名称	定级
1	绵阳市肿瘤医院HIS系统	2级
2	绵阳市肿瘤医院LIS系统	2级
3	绵阳市肿瘤医院PACS系统	2级
4	绵阳市肿瘤医院EMR系统	2级
5	绵阳市肿瘤医院门户网站	2级
6	同时针对HIS系统、电子病历系统进行渗透测试，开展一次攻防演练，出具演练报告，以及网络安全培训一次	1

（二）项目需求

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度，以及云计算安全、移动互联安全、物联网安全、工控制系统安全等扩展方面的要求。

具体服务内容包括：

（1）协助业主单位进行信息系统的信息安全等级定级和备案工作。

（2）差距测评，至少包括：

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、安全系统建设和安全系统运维五个方面的安全测评。

形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以、整改意见。

（3）协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

（4）等级测评，至少包括：

按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。

（三）服务内容指标

1.二级系统通用指标要求

分类	子类	基本要求
安全物理环境	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内; b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识; b) 应将通信线缆铺设在隐蔽安全处。
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火; b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透; b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备; b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。

		安全通信网络	网络架构	a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址; b) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
			通信传输	应采用校验技术保证通信过程中数据的完整性。
			可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信 验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
		安全区域边界	边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
			访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信; b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化; c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出; d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
			入侵防范	应在关键网络节点处监视网络攻击行为。
			恶意代码防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
			安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计; b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息; c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
			可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行 可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
			身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换; b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施; c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
			访问控制	a) 应对登录的用户分配账户和权限; b) 应重命名或删除默认账户，修改默认账户的默认口令; c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在; d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

		安全计算环境	安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计; b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息; c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。
			入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序; b) 应关闭不需要的系统服务、默认共享和高危端口; c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制; d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求; e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
			恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
			可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
			数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
			数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能; b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
			剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
			个人信息保护	a) 应仅采集和保存业务必需的用户个人信息; b) 应禁止未授权访问和非法使用用户个人信息。
		安全管理中心	系统管理	a)应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对 这些操作进行审计; b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、 系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
			审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计; b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
			安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全 框架等。

	1	安全管理制度	管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度; b) 应对管理人员或操作人员执行的日常管理操作建立操作规程。
			制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定; b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
			评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制 度进行修订。
		安全管理机构	岗位设置	a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责; b) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
			人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
			授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等; b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。
			沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题; b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通; c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
			审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
		安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用; b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查。
			人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设 备。
			安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。
			外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案; b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案; c) 外部人员离场后应及时清除其所有的访问权限。
			定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由; b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定; c) 应保证定级结果经过相关部门的批准; d) 应将备案材料报主管部门和相应公安机关备案。

			安全建设管理	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施; b) 应根据保护对象的安全保护等级进行安全方案设计; c) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后 才能正式实施。
				产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定; b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
				自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制; b) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
				外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码; b) 应保证开发单位提供软件设计文档和使用指南。
				工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理; b) 应制定安全工程实施方案控制工程实施过程。
				测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告; b) 应进行上线前的安全性测试，并出具安全测试报告。
				系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点; b) 应对负责运行维护的技术人员进行相应的技能培训; c) 应提供建设过程文档和运行维护文档。
				等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改; b) 应在发生重大变更或级别发生变化时进行等级测评; c) 应确保测评机构的选择符合国家有关规定。
				服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定; b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
				环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理; b) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等; c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
				资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
				介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点; b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

			安全运维管理	设备维护管理	a) 应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理; b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
				漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响 后进行修补。
				网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限; b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制; c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面做出规定; d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等; e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
				恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等; b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等; c) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
				配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和 补丁信息、各个设备或软件组件的配置参数等。
				密码管理	a) 应遵循密码相关国家标准和行业标准; b) 应使用国家密码管理主管部门认证核准的密码技术和产品。
				变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。
				备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等; b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等; c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
				安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件; b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等; c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
				应急预案管理	a) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容; b) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

	外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定; b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

2.二级系统扩展指标要求

云计算安全扩展要求

分类	子类	基本要求
安全物理环境	基础设施位置	应保证云计算基础设施位于中国境内。
安全通信网络	网络架构	a) 应保证云计算平台不承载高于其安全保护等级的业务应用系统; b) 应实现不同云服务客户虚拟网络之间的隔离; c) 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
安全区域边界	访问控制	a) 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则; b) 应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。
	入侵防范	a) 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等; b) 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等; c) 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
	安全审计	a) 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启; b) 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。
安全计算环境	访问控制	a) 应保证当虚拟机迁移时，访问控制策略随其迁移; b) 应允许云服务客户设置不同虚拟机之间的访问控制策略。
	镜像和快照保护	a) 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务; b) 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。
	数据完整性和保密性	a) 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定; b) 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限; c) 应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
	数据备份恢复	a) 云服务客户应在本地保存其业务数据的备份; b) 应提供查询云服务客户数据及备份存储位置的能力。
	剩余信息保护	a) 应保证虚拟机所使用的内存和存储空间回收时得到完全清除; b) 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。
安全管理中心	等保二级无	等保二级无

安全建设管理	云服务商选择	a) 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力； b) 应在服务水平协议中规定云服务的各项服务内容和具体技术指标； c) 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等； d) 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。
	供应链管理	a) 应确保供应商的选择符合国家有关规定； b) 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户。
安全运维管理	云计算环境管理	云计算平台的运维地点应位于中国境内，非国内对境内云计算平台实施运维操作应遵循国家相关规定。

（四）完成项目所需提交的文档清单

在本项目完成后，服务方须提供以下文档资料：

1.《信息系统安全问题汇总及整改建议》

2.《网络安全等级保护等级测评报告》及过程资料

3.《渗透测试报告》

4.《攻防演练报告》

（五）技术标准和规范

1.《中华人民共和国计算机信息系统安全保护条例》(国务院令147号)

2.《信息安全等级保护管理办法》（公通字[2007]43号

3.《计算机信息系统安全保护等级划分准则》（GB17859-1999）

4.《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）

5.《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019)

6.《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）

7.《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）

8.《信息安全技术信息安全风险评估方法》（GB/T20984-2022）

（六）安全要求

成交供应商在项目实施过程中，必须遵守以下技术原则：

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。

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.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，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

4.可控性原则：等保测评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：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及的各个层面。

6.安全性原则：等保测评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。

7.测评机构资质及人员要求：

		从事信息系统检测评估相关工作人员无违法记录。 工作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。 测评期间需遵守被测单位相关管理规定，禁止利用测评工作从事危害被测单位利益、安全的活动。

3.2.3人员配置要求

采购包1：

满足项目实施需要。

采购包2：

满足项目实施需要。

3.2.4设施设备要求

采购包1：

满足项目实施需要。

采购包2：

满足项目实施需要。

3.2.5其他要求

采购包1：

满足项目实施需要。

采购包2：

满足项目实施需要。

3.3、商务要求

3.3.1服务期限

采购包1：

自合同签订之日起30日

采购包2：

自合同签订之日起30日

3.3.2服务地点

采购包1：

采购人指定地点

采购包2：

采购人指定地点

3.3.3考核（验收）标准和方法

采购包1：

中标人与采购人应严格按照按国家有关规定、采购文件的服务要求、成交供应商响应文件及承诺以及合同约定标准及根据《政府采购需求管理办法》（财库〔2021〕22号）文件的规定，同时参照《四川省政府采购项目需求论证和履约验收管理办法》（财库〔2016〕205号）文件的要求及国家行业主管部门规定的标准、方法和内容组织验收。

采购包2：

中标人与采购人应严格按照按国家有关规定、采购文件的服务要求、成交供应商响应文件及承诺以及合同约定标准及根据《政府采购需求管理办法》（财库〔2021〕22号）文件的规定，同时参照《四川省政府采购项目需求论证和履约验收管理办法》（财库〔2016〕205号）文件的要求及国家行业主管部门规定的标准、方法和内容组织验收。

3.3.4支付方式

采购包1：

分期付款

采购包2：

一次付清

3.3.5支付约定

采购包1： 付款条件说明： 合同签订后，中标人开具发票后 ，达到付款条件起 10 日内，支付合同总金额的 30.00%。

采购包1： 付款条件说明： 项目竣工经验收合格后 ，达到付款条件起 10 日内，支付合同总金额的 70.00%。

采购包2： 付款条件说明： 甲方在收到乙方出具的《信息系统安全等级保护测评报告》并顺利通过验收后 ，达到付款条件起 30 日内，支付合同总金额的 100.00%。

3.3.6违约责任及解决争议的方法

采购包1：

签订合同时约定

采购包2：

签订合同时约定

3.4其他要求

无

第四章 磋商过程中可实质性变动的内容

磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第七章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

第五章 磋商办法

5.1总则

一、根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购竞争性磋商采购方式管理暂行办法》《四川省政府采购评审工作规程（修订）》等法律规章，结合本采购项目特点制定本次竞争性磋商评审方法。

二、评审工作由代理机构组织，具体评审事务由依法组建的磋商小组负责。

三、评审工作应遵循客观、公正、审慎的原则，并以相同的磋商程序和标准对待所有的供应商。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。磋商小组成员、采购人、代理机构和供应商应当按照本磋商文件规定和项目电子化交易系统操作要求开展或者参加评审活动。

五、评审过程中的书面材料往来均通过项目电子化交易系统传递，评审委员会成员使用互认的证书及签章进行签名后生效，供应商通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评审委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评审过程应当独立、保密，任何单位和个人不得非法干预评审活动。供应商非法干预评审活动的，其响应文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评审活动的，将依法追究其责任。

5.2 磋商小组

一、本项目磋商小组成员人数应为三人以上单数，其中评审专家不得少于成员总数的三分之二。评审专家是采取随机方式在采购一体化平台的专家库系统（以下简称专家库系统）抽取。技术复杂、专业性较强的采购项目，评审专家中应当包含1名法律专家。

二、磋商小组成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐磋商小组组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、磋商小组成员获取解密后的响应文件，开展评审活动。出现应当回避的情形时，磋商小组成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商响应文件，按规定重新组建磋商小组，解封响应文件后，开展评审活动。

四、磋商小组按照磋商文件规定的磋商程序、评分方法和标准进行评审，并独立履行下列职责：

（一）熟悉和理解磋商文件；

（二）审查供应商响应文件等是否满足磋商文件要求，并作出评价；

（三）根据需要要求采购组织单位对磋商文件作出解释；根据需要要求供应商对响应文件有关事项作出澄清、说明或者更正；

（四）推荐成交候选供应商，或者受采购人委托确定成交供应商；

（五）起草资格审查报告、评审报告并进行签署；

（六）向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为；

（七）法律、法规和规章规定的其他职责。

5.3评审程序

5.3.1.熟悉和理解磋商文件和停止评审

一、磋商小组正式评审前，应当对磋商文件进行熟悉和理解，内容主要包括磋商文件中供应商资格条件要求、采购项目技术、服务和商务要求、磋商办法和标准、政府采购政策要求以及政府采购合同主要条款等。

二、本磋商文件有下列情形之一的，磋商小组应当停止评审：

（一）磋商文件的规定存在歧义、重大缺陷的；

（二）磋商文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；

（三）采购项目属于国家规定的优先、强制采购范围，但是磋商文件未依法体现优先、强制采购相关规定的；

（四）采购项目属于政府采购促进中小企业发展的范围，但是磋商文件未依法体现促进中小企业发展相关规定的；

（五）磋商文件将供应商的资格条件列为评分因素的；

（六）磋商文件载明的成交原则不合法的；

（七）磋商文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评审情形的，磋商小组应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，磋商小组不得以任何方式和理由停止评审。

出现上述应当停止评审情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在四川政府采购网公告。采购组织单位认为磋商小组不应当停止评审的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

5.3.2资格审查

响应文件提交截止时间结束后，由磋商小组依据法律法规和磋商文件的规定，对响应文件中的资格证明等进行审查，以确定供应商是否具备响应资格，并出具资格审查报告。资格审查标准及要求如下：

响应文件提交截止时间结束后，由磋商小组依据法律法规和磋商文件的规定，对响应文件中的资格证明等进行审查，以确定供应商是否具备响应资格，并出具资格审查报告。资格审查标准及要求如下：

5.3.2.1一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	具有独立承担民事责任的能力。	1）供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。（2）1.供应商为企业（包括合伙企业）、个体工商户的,应提供工商营业执照或提供由市场监管部门核发的法人或者其他组织统一社会信用代码的营业执照（扫描件）；2.供应商属于银行、保险、石油石化、电力、电信等有行业特殊情况的，提供企业分支机构营业执照或统一社会信用代码的营业执照（扫描件）；3.供应商为其他组织的，提供事业单位法人证书或执业许可证等证明文件（扫描件）；4.如为自然人的提供《中华人民共和国居民身份证》（扫描件，持原件备查）。	响应文件封面 供应商应提交的相关资格证明材料 投标（响应）函
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

3	具有健全的财务会计制度。	供应商是否有健全的财务会计制度（提供以下任意一项均可）：①供应商2020年至2022年中任意一年的经审计的财务报告，至少包括“三表一注”，即资产负债表、利润表、现金流量表及其附注（复印件，加盖供应商鲜章）；②属于银行、保险、石油石化、电力、电信等有行业特殊情况的，提供2020年至2022年中任意一年的财务报表（复印件扫描件，加盖供应商鲜章）；③新成立的公司不足1年或非公司性质的供应商提供银行的资信证明（复印件扫描件，加盖供应商鲜章）；④提供具有健全的财务会计制度承诺函（原件扫描件）。	供应商应提交的相关资格证明材料 投标（响应）函
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式

1	具有独立承担民事责任的能力。	1）供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。（2）1.供应商为企业（包括合伙企业）、个体工商户的,应提供工商营业执照或提供由市场监管部门核发的法人或者其他组织统一社会信用代码的营业执照（扫描件）；2.供应商属于银行、保险、石油石化、电力、电信等有行业特殊情况的，提供企业分支机构营业执照或统一社会信用代码的营业执照（扫描件）；3.供应商为其他组织的，提供事业单位法人证书或执业许可证等证明文件（扫描件）；4.如为自然人的提供《中华人民共和国居民身份证》（扫描件，持原件备查）。	响应文件封面 供应商应提交的相关资格证明材料 投标（响应）函
2	具有良好的商业信誉	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
3	具有健全的财务会计制度。	供应商是否有健全的财务会计制度（提供以下任意一项均可）：①供应商2020年至2022年中任意一年的经审计的财务报告，至少包括“三表一注”，即资产负债表、利润表、现金流量表及其附注（复印件，加盖供应商鲜章）；②属于银行、保险、石油石化、电力、电信等有行业特殊情况的，提供2020年至2022年中任意一年的财务报表（复印件扫描件，加盖供应商鲜章）；③新成立的公司不足1年或非公司性质的供应商提供银行的资信证明（复印件扫描件，加盖供应商鲜章）；④提供具有健全的财务会计制度承诺函（原件扫描件）。	供应商应提交的相关资格证明材料 投标（响应）函
4	具有履行合同所必需的设备和专业技术能力。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
5	有依法缴纳税收和社会保障资金的良好记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
6	参加政府采购活动前三年内，在经营活动中没有重大违法记录。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

7	不存在与单位负责人为同一人或者存在直接控股、管理关系的其他供应商参与同一合同项下的政府采购活动的行为。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函
8	不属于为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商。	供应商需在项目电子化交易系统中按要求填写《投标（响应）函》完成承诺并进行电子签章。	投标（响应）函

5.3.2.2特殊资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。	参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。	无行贿犯罪记录的承诺函 投标（响应）函

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。	参加本次政府采购活动前三年内，投标人单位及其现任法定代表人不得具有行贿犯罪记录。	无行贿犯罪记录的承诺函 投标（响应）函
2	具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》	具备公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》	供应商应提交的相关资格证明材料 投标（响应）函

5.3.2.3落实政府采购政策资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包属于专门面向中小企业采购。	供应商结合自身实际，按照采购文件要求和关联格式要求，提供《中小企业声明函》或者《残疾人福利性单位声明函》、《监狱企业证明文件》进行响应。	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包属于专门面向中小企业采购。	供应商结合自身实际，按照采购文件要求和关联格式要求，提供《中小企业声明函》或者《残疾人福利性单位声明函》、《监狱企业证明文件》进行响应。	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

5.3.3磋商

一、 磋商小组按照磋商文件的规定与邀请参加磋商的供应商分别进行磋商，磋商顺序由磋商小组确定。

二、 磋商小组所有成员集中与单一供应商对技术、服务、合同条款等内容分别进行一轮或多轮的磋商。在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

三、磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第六章“拟签订的合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

四、 对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应通过项目电子化交易系统，将变动情况通知本轮次所有参加磋商的供应商。磋商过程中，磋商小组可以根据磋商情况调整磋商轮次。

五、 磋商过程中，供应商可以根据磋商情况变更其响应文件，并将变更内容以“供应商响应表”形式在线提交磋商小组。“供应商响应表”作为响应文件的一部分，应加盖供应商（法定名称）电子印章，否则无效。

六、经最终磋商后，响应文件仍有下列情况之一的，应按照无效响应处理：

（一）响应文件仍不能实质响应磋商文件可实质性变动的实质性要求的；

（二）响应文件中仍有磋商文件规定的其他无效响应情形的。

七、 磋商过程中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

八、 磋商过程中，磋商小组发现或者知晓供应商存在违法行为的，应当磋商报告中予以记录，并向本级财政部门报告，依法应将该供应商响应文件作无效处理的，应当作无效处理。

5.3.4符合性审查

磋商小组依据本磋商文件的实质性要求，对符合资格的响应文件进行审查，以确定其是否满足本磋商文件的实质性要求。本项目的符合性审查事项必须以本磋商文件的明确规定的实质性要求为依据。

在符合性审查过程中，如果出现磋商小组成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和磋商文件规定。

符合性审查标准见下表：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	1.在磋商过程中，磋商小组认为供应商报价低于最高限价50%或者低于其他有效供应商报价算术平均价40%，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在评审现场合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就供应商提供的货物、工程和服务的主营业务成本（应根据供应商企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。 2.供应商提交的相关证明材料，应当加盖供应商（法定名称）电子印章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。供应商不能证明其报价合理性的，磋商小组应当将其响应文件作为无效处理。	分项报价表 商务应答表 服务内容及服务要求应答表 报价表

采购包2：

序号	符合审查要求概况	评审点具体描述	关联格式

1	不正当竞争预防措施（实质性要求）	1.在磋商过程中，磋商小组认为供应商报价低于最高限价50%或者低于其他有效供应商报价算术平均价40%，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在评审现场合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就供应商提供的货物、工程和服务的主营业务成本（应根据供应商企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。 2.供应商提交的相关证明材料，应当加盖供应商（法定名称）电子印章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。供应商不能证明其报价合理性的，磋商小组应当将其响应文件作为无效处理。	分项报价表 商务应答表 服务内容及服务要求应答表 报价表

5.3.5最后报价

一、方案评审

采购包1：磋商结束后，磋商小组可以根据磋商情况要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。如本项目属于政府购买服务项目（含政府和社会资本合作项目)、市场竞争不充分的科研项目或者需要扶持的科技成果转化项目，提交最后报价的供应商可以为2家。有效最后报价的供应商不足的，本次采购活动终止，并发布终止公告。

采购包2：磋商结束后，磋商小组可以根据磋商情况要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于3家。如本项目属于政府购买服务项目（含政府和社会资本合作项目)、市场竞争不充分的科研项目或者需要扶持的科技成果转化项目，提交最后报价的供应商可以为2家。有效最后报价的供应商不足的，本次采购活动终止，并发布终止公告。

二、磋商小组开启报价后，供应商应随时关注项目电子化交易系统信息提醒，登录项目电子化交易系统，通过“等候大厅”进行报价并签章后提交。

三、供应商在未提高响应文件中承诺的标准情况下，其最后报价不得高于对该项目之前的报价，否则，磋商小组将对其响应文件作无效处理，并通过电子化交易系统告知供应商，说明理由。

四.供应商未在响应文件提交截止时间内提交报价或未按要求进行报价的，视为无效响应，由供应商自行承担不利后果。

五、供应商未按磋商小组要求在规定时间内提交最后报价的，视为其退出磋商。

六、最后报价一旦提交后，供应商不得以任何理由撤回。

七、最后报价为有效报价应符合下列条件：

（一）供应商所提供的最后报价是在规定的时间内提交。

（二）供应商的最后报价应加盖供应商（法定名称）电子印章。

（三）供应商的最后报价应符合磋商文件的要求。

（四）最后报价唯一，且不高于最高限价。

八、最后报价出现下列情况的，不需要供应商澄清，按以下原则处理：

（一）报价中的大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；

（二）单价金额小数点或者百分比有明显错位的，应以总价为准，并修改单价；

（三）总价金额与按单价汇总金额不一致的，以单价汇总金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的最后报价经加盖供应商（法定名称）电子印章后产生约束力，供应商不确认的，其最后报价无效。

5.3.6解释、澄清有关问题

一、评审过程中，磋商小组认为磋商文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变磋商文件的原义或者影响公平、公正，解释事项如果涉及供应商权益的以有利于供应商的原则进行解释。

二、对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组应当要求供应商作出必要的澄清、说明或更正，并给予供应商必要的反馈时间。供应商应当按磋商小组的要求进行澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。澄清不影响响应文件的效力，有效的澄清、说明或者更正材料是响应文件的组成部分。

三、供应商的澄清、说明或者更正需进行电子签章，应当不超出响应文件的范围、不实质性改变响应文件的内容、不影响供应商的公平竞争、不导致响应文件从不响应磋商文件变为响应磋商文件的条件。下列内容不得澄清：

（一）供应商响应文件中不响应磋商文件规定的技术参数指标和商务应答；

（二）供应商响应文件中未提供的证明其是否符合磋商文件资格、符合性规定要求的相关材料。

（三）供应商响应文件中的材料因印刷、影印等不清晰而难以辨认的。

四、响应文件报价出现前后不一致的情形，按照本章前述规定予以处理，不需要供应商澄清。

五、代理机构宣布评审结束之前，供应商应通过项目电子化交易系统随时关注评审消息提示，及时响应磋商小组发出的澄清、说明或更正要求。供应商未能及时响应的，自行承担不利后果。

六、磋商小组应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.3.7比较与评价

磋商小组应当按照磋商文件规定的评标细则及标准，对符合性检查合格的响应文件进行商务和技术评估，综合比较和评价。

5.3.8复核

评审结束后，磋商小组应当进行复核，特别要对拟推荐为成交候选供应商的、报价最低的、响应文件被认定为无效的进行重点复核。

评审结果汇总完成后，磋商小组拟出具磋商报告前，代理机构应当组织2名以上的工作人员，在采购现场监督人员的监督之下，依据有关的法律制度和磋商文件对评审结果进行复核，出具复核报告。代理机构复核过程中，磋商小组成员不得离开评审现场。

除资格检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者代理机构不得以任何理由组织重新评审。采购人、代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

5.3.9推荐成交候选供应商

采购包1： 确定3家供应商为成交候选人。

采购包2： 确定3家供应商为成交候选人。

“本项目”磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐成交候选供应商，并编写磋商报告（若本项目属于政府购买服务项目（含政府和社会资本合作项目）/市场竞争不充分的科研项目/需要扶持的科技成果转化项目，当提交最后报价的供应商为2家时，可以推荐2家成交候选供应商）。

评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣（本项目的技术指标为：技术参数要求 ，按照技术指标得分确定优劣）顺序推荐。评审得分且最后报价且技术指标得分均相同的，按供应商根据第六章强制、优先采购产品承诺函格式要求承诺提供的经认证的优先采购节能、环境标志产品数量由多到少顺序推荐。评审

得分、最后报价、技术指标得分和承诺提供的经认证优先采购节能、环境标志产品数量均相同的，成交候选供应商并列。

5.3.10编写磋商报告

磋商小组推荐成交候选供应商后，应向代理机构出具磋商报告。磋商报告应当包括以下主要内容：

（一）邀请供应商参加采购活动的具体方式和相关情况；

（二）响应文件开启日期和地点；

（三）获取磋商文件的供应商名单和磋商小组成员名单；

（四）评审情况记录和说明，包括对供应商响应文件审查情况、磋商情况、报价情况等；

（五）提出的成交候选供应商的排序名单及理由。

磋商报告应当由磋商小组全体人员签字或加盖电子签章认可。磋商小组成员对磋商报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对磋商报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组记录相关情况。磋商小组成员拒绝在磋商报告上签字或加盖电子签章又不书面说明其不同意见和理由的，视为同意磋商报告。

5.3.11评审争议处理规则

在磋商过程中，对于符合性审查、对响应文件作无效响应处理的及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背磋商文件规定。持不同意见的磋商小组成员应当在磋商报告中签署不同意见及理由，否则视为同意评审报告。持不同意见的磋商小组成员认为认定过程和结果不符合法律法规或者磋商文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理。

5.4评审办法及标准

一、磋商小组只对通过资格审查的响应文件，根据磋商文件的要求采用相同的评审程序、评分办法及标准进行评价和比较。

二、磋商小组成员应依据磋商文件规定的评分标准和方法独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

5.4.1评分办法

本次评审采用综合评分法，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

5.4.2评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审70.00分 报价得分30.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

详细评审	技术参数要求	1、完全符合招标文件要求没有负偏离得45分； 2、投标人投标产品★的技术参数必须满足招标文件技术参数要求，不满足为无效投标。 3、招标文件中加▲号的技术参数为重要参数，满足招标文件中的重要参数的得27.4分，每有一项不满足扣1.3分，共21条，扣完为止。 4、完全满足招标文件中其他的技术参数及要求的得17.6分，每有一项不满足扣0.4分，共44条，扣完为止。 重要参数“▲”项须提供技术支持材料：（技术支持材料是指：具有国家认可的第三方机构出具的检测报告、图片、技术白皮书、彩页等证明材料加盖供应商鲜章），未按要求提供佐证材料或不满足按评分标准要求扣分。	45.00	客观	供应商认为需要提供的其他证明材料 商务应答表
	售后服务	供应商根据本项目特点提供的售后服务方案进行评审，内容包含但不限于：①工作目标和范围；②实施流程；③实施计划；④项目组织架构；⑤项目验收标准。以上五个方面内容完整全面、与项目需求吻合、思路清晰、层次结构细化，有具体详细的阐述且符合项目要求的得10分，方案中每有一项内容与本项目无关或涉及的规范标准不符合要求或方案内容与项目不匹配或内容不详实完整或内容有细微错误、瑕疵或存在缺陷的扣1分，每有一项内容缺失的扣2分。	10.00	主观	商务应答表 售后服务
	业绩	投标人近2年类似业绩，每提供一个的得2.5分，最多得5分，可并列。 提供合同或中标通知书原件扫描件。	5.00	客观	供应商类似项目业绩一览表 商务应答表

	履约能力	为保证项目交付质量，项目实施人员具备：（1）中国信息安全测评中心认证颁发的CISP证书（认证方向：CISE信息安全工程师）得4分，没有不得分。（2）具备中国信息安全测评中心颁发的CISP证书(认证方向：DSG数据安全)证书得4分，没有不得分。	8.00	客观	供应商认为需要提供的其他证明材料 商务应答表
	扶持不发达和少数民族地区	供应商为不发达地区或少数民族地区企业的，得2分。 注：提供为不发达地区企业或注册地为少数民族地区的相关证明材料并加盖供应商公章。	2.00	客观	商务应答表
价格分	价格分	以本次有效的最低投标报价为基准价，投标报价得分=(基准价／投标报价)* 30分*100%	30.00	客观	报价表 分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

采购包2：

评审因素		评审标准			
分值构成		详细评审80.00分 报价得分20.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	综合实力	1.供应商具有质量体系认证证书，得2分； 2.供应商具有信息安全管理系统认证证书，得2分； 3.供应商具有环境管理体系认证证书，得2分； 4.供应商具有职业健康安全管理系统认证证书，得2分； 5.供应商具有中国合格评定国家认可委员会（CNAS）颁发的实验室认可证书，得2分； 注：提供证书复印件加盖公章	10.00	客观	供应商认为需要提供的其他证明材料 商务应答表
	业绩	供应商自2020年1月1日至今每有一个等保测评案例得1分，最多得10分,没有的不得分。 注：提供相关合同复印件加盖公章。	10.00	客观	供应商类似项目业绩一览表

详细评审	履约能力	1.项目组负责人具有以下资格的：项目负责人具有网络安全等级测评师高级证书、互联网安全评估师高级证书（CIISA）、信息安全工程师证书（软考类）、国际软件测试工程师（ISTQB）证书、商用密码应用安全性评估人员能力合格证书、注册云安全系统认证专家（CCSSP）证书的，国家重要信息系统保护人员证书的（CIIPT），实验室质量管理师证书，每项得2分，没有的不得分，此项最多得16分。 2.项目组除负责人外的其它测评人员具有以下资格的： 2.1现场经理具有具有信息安全等级测评师高级证书、注册信息安全专业人员证书（CISP）、工业和信息化部教育与考试中心的网络工程师（高级）、软件性能测评师高级、系统架构师（高级）全部满足得10分，缺少一项扣2分； 2.2其余测评人员具有IT服务工程师（ITSE）证书、互联网安全评估师证书（CIISA）、商用密码应用安全性评估人员能力合格证书、国际软件测试工程师（ISTQB）证书、信息安全保障人员认证证书（CISAW）、国家网络安全应用检测专业测评人员证书（NSATP-A），每项得2分（每项证书不能重复得分），没有的不得分，此项最多得12分。 注：提供相关人员证书证明材料和复印件，加盖公章。	38.00	客观	供应商类似项目业绩一览表

	测评方案	供应商根据本项目特点提供的测评方案进行评审，内容包含但不限于：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、安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维管理。以上10个方面内容完整全面、与项目需求吻合、思路清晰、层次结构细化，有具体详细的阐述且符合项目要求的得20分，方案中每有一项内容与本项目无关或涉及的规范标准不符合要求或方案内容与项目不匹配或内容不详实完整或内容有细微错误、瑕疵或存在缺陷的扣1分，每有一项内容缺失的扣2分。	20.00	主观	供应商认为需要提供的其他证明材料
	扶持不发达和少数民族地区	供应商为不发达地区或少数民族地区企业的，得2分。 注：提供为不发达地区企业或注册地为少数民族地区的相关证明材料并加盖供应商公章。	2.00	客观	商务应答表
价格分	价格分	以本次有效的最低投标报价为基准价，投标报价得分=(基准价／投标报价)* 20分*100%(保留小数点后两位)	20.00	客观	报价表 分项报价表

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

说明：

1、所有的评分、价格等涉及小数计算，先四舍五入再计算；

2、评分标准中要求提供的证明材料须清晰可辨。

5.5终止采购活动

出现下列情形之一的，采购人或者代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

（一）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

（二）出现影响采购公正的违法、违规行为的；

（三）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足3家的（财政部另有规定的除外）；

（四）法律法规规定的其他情形。

5.6确定成交供应商

一、评审结束后，代理机构在评审结束后2个工作日内将磋商报告送采购人。

二、采购人在收到磋商报告后5个工作日内，在磋商报告确定的成交候选供应商名单中按顺序确定1名成交供应商。采购人逾期未确定成交供应商且不提出异议的，视为确定磋商报告提出的排序第一的供应商为成交供应商。

三、采购人或者代理机构应当自成交供应商确定之日起 2 个工作日内，在四川政府采购网上公告成交结果，磋商文件应当随成交结果同时公告。

5.7评审专家在政府采购活动中承担以下义务

（一）遵守评审工作纪律；

（二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；

（三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；

（四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；

（五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；

（六）配合答复处理供应商的询问、质疑和投诉等事项；

（七）法律、法规和规章规定的其他义务。

5.8评审专家在政府采购活动中应当遵守以下工作纪律

（一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。

（二）评审前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。

（三）评审过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的， 应当在监督人员监督之下办理。

（四）评审过程中，不得干预或者影响正常评审工作，不得发表倾向性、引导性意见， 不得修改或细化磋商文件确定的评审程序、评审方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评审意见，不得拒绝对自己的评审意见签字确认。

（五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，除因履行《四川省政府采购评审工作规程（修订）》（川财采〔2016〕53号）第十三条第（六）项规定的义务外，不得向外界透露评审内容。

（六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。

（七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

第六章 响应文件格式

采购包1：

分册名称：投标响应文件分册

详见附件：响应文件封面

详见附件：投标（响应）函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：供应商应提交的相关资格证明材料

详见附件：商务应答表

详见附件：报价表

详见附件：分项报价表

详见附件：服务内容及服务要求应答表

详见附件：售后服务

详见附件：供应商认为需要提供的其他证明材料

详见附件：供应商类似项目业绩一览表

详见附件：无行贿犯罪记录的承诺函

采购包2：

分册名称：投标响应文件分册

详见附件：响应文件封面

详见附件：投标（响应）函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：供应商应提交的相关资格证明材料

详见附件：商务应答表

详见附件：报价表

详见附件：分项报价表

详见附件：服务内容及服务要求应答表

详见附件：供应商类似项目业绩一览表

详见附件：供应商认为需要提供的其他证明材料

详见附件：无行贿犯罪记录的承诺函

政府采购合同（服务类）

政府采购合同编号：_____

履约地点：_____

签订日期：20___年___月___日

签订地点：_____

采购人（甲方）：_____

地址：_____

供应商(乙方)：_____

地址：_____

依据《中华人民共和国民法典》《中华人民共和国政府采购法》与项目行业有关的法律法规，以及XXX采购项目的 《磋商文件》，乙方的《投标（响应）文件》及《中标（成交）通知书》，甲乙双方同意签订本合同。具体情况及要求如下

一、标的信息

二、服务要求

三、合同定价方式、付款进度和支付方式

四、履约保证金

五、验收标准和方法

六、甲方的权利和义务

1.甲方有权对合同规定范围内乙方的服务行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分XXX。

2.根据本合同规定，按时向乙方支付应付服务费用。

3.国家法律、法规所规定由甲方承担的其它责任。

……

七、乙方的权利和义务

1.根据本合同的约定向甲方收取相关服务费用。

2.接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。

3.国家法律、法规所规定由乙方承担的其它责任。

……

八、违约责任

1.若甲方未按照合同约定逾期向乙方支付货物费用，每逾期一天，按应支付金额的X‰作为违约金支付给乙方，直至实际支付之日

2.因甲方原因导致变更、中止或者终止政府采购合同的，应对乙方受到的损失予以赔偿或者补偿。

……

九、不可抗事件处理

1.在合同有效期内，任何一方因战争、洪灾、台风、地震等不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力事件影响期相同。

2.受阻一方应在不可抗力事件发生后尽快用电话通知对方并于事故发生后XX天内将有关部门出具的证明文件等用特快专递或挂号信寄给对方审阅确认。

3.不可抗力事件延续XX天以上，双方应通过友好协商，确定是否继续履行合同

……

十、解决合同纠纷的方式

十一、合同生效及其他

1.合同经双方法定代表人（或主要负责人）或授权委托代理人签字并加盖公章后生效。

2.政府采购合同履行中，甲方需追加与合同标的相同的货物的，在不改变合同其他条款的前提下，可以与乙方协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。补充协议签订后，报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

3.本合同一式3份，自双方签章之日起生效。甲方持有1份，乙方持有1份，同级财政部门备案1份，具有同等法律效力。

甲方：（盖章）　　乙方：(盖章）

法定（授权）代表人：　　法定（授权）代表人：

地 址：　　地 址：

开户银行：　　开户银行：

账号：	账号：
签订日期： 年 月 日	签订日期： 年 月 日