

采购项目编号：SCZD2025-CS-2164/001

陕西省结核病防治院网络安全等级保护测 评项目

竞争性磋商文件

陕西省采购招标有限责任公司

2025年08月

目 录

第一章	磋商公告	2
第二章	供应商须知	7
第三章	评审办法和标准	20
第四章	拟签订的合同文本	31
第五章	采购内容及要求	31
第六章	磋商响应文件格式	54

第一章 竞争性磋商公告

项目概况

陕西省结核病防治院网络安全等级保护测评项目的潜在供应商应在中招联合招标采购平台获取采购文件，并于2025年09月09日09时30分（北京时间）前提交响应文件。

一、项目基本情况

项目编号：SCZD2025-CS-2164/001

项目名称：陕西省结核病防治院网络安全等级保护测评项目

采购方式：竞争性磋商

预算金额：330000.00 元

采购需求：

合同包 1(陕西省结核病防治院网络安全等级保护测评项目)：

合同包预算金额：330000.00 元

品目号	品目名称	采购标的	数量（单位）	技术规格、参数及要求	品目预算（元）	最高限价（元）
1-1	计算机设备维修和保养服务	网络安全等级保护测评服务项目	1(套)	见采购文件	330000.00	330000.00

本合同包不接受联合体投标

合同履行期限：自各标的提供服务后一年内。

二、申请人的资格要求：

1. 满足《中华人民共和国政府采购法》第二十二条规定；
2. 落实政府采购政策需满足的资格要求：

合同包 1(陕西省结核病防治院网络安全等级保护测评项目)落实政府采购政策需满

足的资格要求如下:无

3. 本项目的特定资格要求:

合同包 1(陕西省结核病防治院网络安全等级保护测评项目)特定资格要求如下:

3.1 供应商参加本项目的合法授权人授权委托书; 供应商应授权合法的人员参加投标全过程, 其中法定代表人直接参加磋商的, 须出具法人身份证, 并与营业执照上信息一致。法定代表人授权代表参加磋商的, 须出具法定代表人授权书及授权代表身份证、授权代表本单位证明(提供授权代表在本单位养老保险缴纳证明);

3.2 供应商在递交响应文件截止时间前被“中国执行信息公开网(<http://zxgk.court.gov.cn/shixin/>)”列入失信被执行人、被“信用中国”网站(www.creditchina.gov.cn)列入重大税收违法失信主体、被“中国政府采购网”网址(www.ccgp.gov.cn)上列入政府采购严重违法失信行为信息记录的, 不得参加磋商;

3.3、供应商须具有《网络安全等级测评与检测评估机构服务认证证书》;

3.4 供应商不得存在下列情形之一:

(1) 单位负责人为同一人或者存在直接控股、管理关系的不同供应商, 不得参加本次采购活动;

(2) 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, 不得再参加本项目的采购活动;

3.5 需按照磋商公告要求的方式获取磋商文件并登记备案, 未按磋商公告要求的方式获取磋商文件并登记备案的供应商均无资格参加磋商。

三、获取采购文件

时间: 2025 年 08 月 29 日至 2025 年 09 月 04 日, 每天上午 09:00:00 至 12:00:00, 下午 14:00:00 至 17:00:00 (北京时间, 法定节假日除外)

地点: 中招联合招标采购平台

方式: 在线获取

售价: 500 元

四、响应文件提交

截止时间: 2025 年 09 月 09 日 09 时 30 分 00 秒 (北京时间)

地点: 西安市锦业路 1 号都市之门 C 座九楼第三会议室

五、开启

时间：2025年09月09日09时30分00秒（北京时间）

地点：西安市锦业路1号都市之门C座九楼第三会议室

六、公告期限

自本公告发布之日起3个工作日。

七、其他补充事宜

1、落实政府采购政策：

1.1《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）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）、《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）。

1.2《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）、《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）、《关于印发环境标志产品政府采购品目清单的通知》（财库〔2019〕18号）、《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）。

1.3《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19号）、《关于印发〈关于深入开展政府采购脱贫地区农副产品工作推进乡村产业振兴的实施意见〉的通知》（财库〔2021〕20号）。

1.4《国家互联网信息办公室 工业和信息化部 公安部 财政部 国家认证认可监督管理委员会关于调整网络安全专用产品安全管理有关事项的公告》（2023年第1号）。

1.5《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）、《陕西省财政厅关于印发〈陕西省中小企业政府采购信用融资办法〉的通知》（陕财办采〔2018〕23号）。

1.6《关于扩大政府采购支持绿色建材促进建筑品质提升政策实施范围的通知》（财库〔2022〕35号）、《财政部办公厅 住房城乡建设部办公厅 工业和信息化部办公厅关于印发〈政府采购支持绿色建材促进建筑品质提升政策项目实施指南〉的通知》（财办库〔2023〕52号）。

若享受以上政策优惠的企业，提供相应声明函或品目清单范围内产品的有效认证证书或相关证明。

2. 凡有意参加本项目磋商，登陆中招联合招标采购平台下载电子磋商文件，磋商文件每套售价 500 元，售后不退。下载者请务必至少在文件发售截止时间半个工作日前登录平台完成购买操作，否则将无法保证获取电子磋商文件。若领取纸质版磋商文件的，在获取电子版磋商文件后来我公司领取。

3. 下载者登陆平台前，须前往中招联合招标采购平台：<http://www.365trade.com.cn/>免费注册。

4. 下载者须通过平台填写“购标申请”，并上传法人授权书，否则购买操作无法完成。

5. 下载者需要发票的，须通过平台填写“开票申请”；招标文件费用由招标代理机构出具(将开票信息及付款凭证发送至 20009180@qq.com)，在开标时领取；平台下载服务费、由“中招联合信息股份有限公司”出具增值税电子普通发票，可登录平台自行下载。

6. 平台统一服务热线：010-86397110，（工作日 9:00-12:00，13:30-17:00），平台将确保下载者的购买信息在开标前对平台公司有关工作人员保密；如下载者主动与平台公司工作人员联系咨询事宜，则视为下载者主动放弃信息保密的权利，平台公司将不承担任何责任。

八、对本次招标提出询问，请按以下方式联系。

1、采购人信息

名称：陕西省结核病防治院

地址：陕西省西安市长安区太乙官镇上湾村甲字 1 号

电话：029-85899294

2、采购代理机构信息

名称：陕西省采购招标有限责任公司

地址：西安市锦业路 1 号都市之门 C 座九楼

联系方式：029-88497916

3、项目联系方式

项目联系人：姜凯、雷鹏

电话：029-88497916

第二章 供应商须知

(一) 供应商须知前附表

本表是对供应商须知的具体补充和修改，如有矛盾，均以本表为准。

条款号	内容说明
1.1	项目名称：陕西省结核病防治院网络安全等级保护测评项目 项目编号：SCZD2025-CS-2164/001 最高限价：33 万元
2.1	采购人：陕西省结核病防治院
2.2	采购代理机构：陕西省采购招标有限责任公司
2.3	邀请供应商的方式：发布磋商公告
3.1	对供应商的资格要求：见磋商公告
3.6	是否允许联合体磋商：否
3.7	本项目所属行业：软件和信息技术服务业
12.1	磋商报价：成交响应报价为完成本项目并达到磋商文件要求所需要的全部费用。 (1) 报价货币：人民币； (2) 严格按照分项报价表进行分项报价。
14.1	本项目收取磋商保证金： 供应商向采购代理机构递交人民币 <u>伍仟元</u> （¥5000 元）的磋商保证金。 收取保证金单位名称：陕西省采购招标有限责任公司 开户银行：中国银行西安南郊支行营业部 账号：103260088024 联系人：财务部 联系电话：029-85256853
15.1	磋商有效期：自响应文件递交之日起 <u>60</u> 日历天。
16.1	响应文件的份数：正本 1 份，副本 2 份，电子版 1 份。
17.2	密封袋（箱）上须标注：

条款号	内容说明
	(1) 项目编号： (2) 项目名称： (3) 供应商名称：
18.1	<p>响应文件递交截止时间：2025年09月09日09:30（北京时间）。</p> <p>响应文件递交地点：西安市锦业路1号都市之门C座九楼第三会议室。</p> <p>响应文件须于响应文件递交截止时间之前由专人密封送达响应文件递交地点，以电报、传真、电子邮件形式递交的响应文件将不予接受。</p>
21.1	磋商小组由 <u>3</u> 人组成，其中评审专家 <u>2</u> 人，采购人代表 <u>1</u> 人。
28.1	是否提交履约保证金：否。

(二) 供应商须知

一、总 则

1. 项目说明

1.1 项目说明：见供应商须知前附表。

2. 定义

2.1 采购人：见供应商须知前附表。

2.2 采购代理机构：见供应商须知前附表。

2.3 供应商：指响应磋商文件要求、参加竞争性磋商采购的法人、其他组织或者自然人。本次政府采购项目邀请供应商方式见**供应商须知前附表**。

2.4 磋商小组：指参考《中华人民共和国政府采购法》和财政部《政府采购竞争性磋商采购方式管理暂行办法》有关规定组建，依法依规履行其职责和义务的机构。

3. 合格的供应商

3.1 供应商基本资质要求详见**供应商须知前附表**。

3.2 供应商必须向采购代理机构获取磋商文件，未向采购人或采购代理机构获取磋商文件的潜在供应商均无资格参加本次采购。

3.3 供应商应参考《中华人民共和国政府采购法》及其它有关的中国法律和法规。

3.4 本项目参考《中华人民共和国政府采购法》及其它有关的中国法律和法规。

4. 磋商费用

4.1 供应商应承担所有与编写和提交响应文件有关费用，无论磋商过程和结果如何，采购人在任何情况下均无义务和责任承担这些费用。

二、磋商文件说明

5. 通知

5.1 对与本项目有关的通知，采购人或采购代理机构将以书面（包括书

面材料、信函、传真、电子邮件等，下同）的形式，送达所有与通知有关的已获取了磋商文件的供应商（潜在供应商），传真号码以供应商登记的为准。供应商应于收到通知后按规定时间以书面方式予以回复确认。因登记有误或传真线路故障导致通知延迟送达或无法送达，采购人或采购代理机构不承担责任。

6. 磋商文件的构成

6.1 磋商文件用以阐明供应商所提供的货物以及其它类似的义务、采购响应程序和合同条款。磋商文件包括如下六章内容：

第一章 磋商公告

第二章 供应商须知

第三章 评审办法和标准

第四章 合同草案条款

第五章 采购内容及要求

第六章 磋商响应文件格式

6.2 供应商应认真阅读磋商文件中所有的事项、格式条款和规范要求等。供应商没有对磋商文件做出全面的实质性响应是供应商的风险。采购人有权拒绝没有对磋商文件要求做出实质性响应的响应文件。

7. 磋商文件的澄清和修改

7.1 在首次响应文件递交截止时间前，采购人或采购代理机构可以对已发出的磋商文件进行必要的澄清或修改，澄清或修改的内容为磋商文件的组成部分。

7.2 磋商文件的修改将以书面形式通知所有获取磋商文件的供应商，并对其具有约束力。供应商在收到上述通知后，应立即向采购人回函确认。

7.3 澄清或修改的内容可能影响响应文件编制的，采购人或采购代理机构可适当延长首次响应文件递交截止时间，并以书面形式通知所有获取磋商文件的供应商。

三、响应文件的编写

8. 响应文件语言

8.1 响应文件及与响应相关的所有文件均应以中文书写。

9. 计量单位

9.1 除在磋商文件的技术规格中另有规定外，计量单位应使用中华人民共和国法定计量单位。

10. 响应文件的组成

10.1 供应商编写的响应文件由磋商响应文件组成。供应商应完整地按照磋商文件提供的响应文件格式及要求编写响应文件。响应文件中资格审查和符合性审查涉及的事项不满足要求的，其响应文件将被认定为无效。

10.2 供应商提供的以上材料必须真实有效，任何一项的虚假将导致其响应被拒绝。

11. 响应文件格式

11.1 对于磋商文件第六章中已经提供了格式的响应文件内容，供应商必须按提供的响应文件格式进行填写和编制，没有提供格式的可自行设计。

12. 响应报价

12.1 响应报价应包括供应商为完成磋商文件中规定的本项目采购内容和范围所需要的全部费用，以及与所报服务相关的所有税费，具体包括但不限于第五章列出的内容。供应商估算错误或漏项的风险一律由供应商承担。见**供应商须知前附表**。

12.2 供应商应在响应分项报价表中详细列出所报货物的单价，并由法定代表人或其授权代表签署并加盖公章。响应分项报价表上的价格应按磋商文件第六章的格式填写。

12.3 响应分项报价表的总价应和响应报价一览表的响应报价相一致，也包括供应商为完成本项目所发生的一切费用且已包括与所报服务

相关的所有税费。若响应分项报价表的总价和响应报价一览表的响应报价不一致，则供应商的报价以《响应报价一览表》的响应报价为准。

12.4 供应商的所报单价在合同执行过程中是固定不变的，未经采购人许可不得以任何理由予以变更。以可调整的价格提交的响应文件将作为非实质性响应而予以拒绝。

12.5 供应商对本次服务只允许有一个报价，采购人不接受有任何选择的报价。

12.6 供应商根据本须知 12.2 条规定将响应报价分成几部分并按磋商文件第六章提供的格式填写“响应分项报价表”，只是为了方便采购人对响应文件进行比较，并不限制采购人以其它方式签订合同的权力。

13. 报价货币

12.3 磋商响应函、响应报价一览表、响应分项报价表、最后报价表等所有报价一律用人民币填报。采购人不接受任何非人民币币种的报价。

14. 磋商保证金：见本须知前附表

15. 磋商有效期

15.1 磋商有效期见本须知前附表。在磋商有效期内，所有响应文件均保持有效。响应文件的有效期限比本须知规定的有效期短的，将被视为非实质响应，采购人有权拒绝。

15.2 特殊情况下，采购人可于原磋商有效期满之前要求供应商同意延长有效期，要求与答复均应为书面形式。供应商可以拒绝上述要求，其投标保证金不被没收。对于同意该要求的供应商，既不要求也不允许其修改响应文件，但将要求其相应延长磋商保证金的有效期，有关退还和保证金不予退还的规定在磋商有效期的延长期内继续有效。

16. 响应文件的制作和签署

16.1 供应商应准备一份响应文件正本和“供应商须知前附表”中规定数

目的副本，每套响应文件须清楚地标明“正本”、“副本”、“电子版”。若正本和副本不符，以正本为准。

- 16.2 响应文件须用中文编写，并采用 A4 纸张装订成册。装订须牢固，不易拆散和换页，采用软胶装，不得采用活页方式装订，封面不建议硬装。
- 16.3 响应文件的正本，一律用不褪色的墨水书写或打印，签字页加盖供应商单位公章，并由供应商的法定代表人或其授权的代理人签署。响应文件的副本可采用正本的复印件。
- 16.4 任何行间插字、涂改或增删，必须由响应文件签字人将姓或首字母在旁边签字才有效。
- 16.5 采购人不接受以电报、电话、传真、电子邮件形式递交的响应文件。
- 16.6 供应商在磋商过程中，签订、履行、通知等事项的书面文件中的单位盖章、印章、公章等处均应使用与供应商全称相一致的公章，不得使用其他形式（如带有“专用章”等字样）的印章。如响应过程中供应商使用专用章，须提供特别说明函，明确该专用章作为相关响应文件的盖章，其效力等同于公章（该特别说明函须同时加盖供应商公章和供应商专用章）。
- 16.7 响应文件应按照文件格式制作，并用不可拆装的方式分别装订成册。

四、响应文件的密封和递交

17. 响应文件的密封和标记

- 17.1 供应商应将所有磋商响应文件密封在一个密封袋（箱）中，电子版单独密封，并在密封袋（箱）上标明“磋商响应文件”、“电子版”字样，封口处应加盖公章或授权代表签字。
- 17.2 密封袋（箱）上标识的内容见**供应商须知前附表**。响应文件如果未按上述规定密封和标记，采购代理机构应当拒绝接收。
- 17.3 书面方式不能准确描述采购需求或者需要对样品进行主观判断以确认是否满足采购需求的情况下需提交样品。成交单位样品不予退

还，成为合同内容的一部分，做为验收依据。样品的要求见**供应商须知前附表**。

18. 响应文件递交截止时间

18.1 响应文件递交截止时间和地点见**供应商须知前附表**。

18.2 供应商须由其合法的授权人在响应文件递交截止时间之前将响应文件在响应文件递交地点送达采购人并签字确认。供应商须承担因未送达并签字所造成的一切责任。

18.3 采购人可以按本须知第 7 条规定，通知修改磋商文件，适当延长响应文件递交截止时间。在此情况下，采购人和供应商受响应文件递交截止时间制约的所有权利和义务均应延长至新的截止期。

19. 迟交的响应文件

19.1 采购人将拒绝接收第 18 条规定的响应文件递交截止时间后递交的任何响应文件。

20. 响应文件的修改和撤回

供应商在提交响应文件后可对其响应文件进行修改或撤回，但该修改或撤回的书面通知须在响应文件递交截止时间之前送达响应文件递交地点，且该通知需其法定代表人或经正式授权的供应商代表签字方为有效。

20.1 供应商对响应文件修改的书面材料或撤回的通知应按第 16 和 17 条规定进行编写、密封、标注和递送，并注明“修改响应文件”或“撤回响应文件”字样。

20.2 在响应文件递交截止时间之后，供应商不得对其响应文件做任何修改。

20.3 供应商不得在响应文件递交截止时间起至响应文件有效期期满前撤销其响应文件。

五、评审与磋商

21. 磋商小组

21.1 在磋商开始前组建磋商小组，磋商小组由采购人代表和有关专家组成。专家从政府采购评审专家库相关专业中随机抽取。磋商小组组成见**供应商须知前附表**。

21.2 磋商小组职责

- (1) 确认竞争性磋商文件；
- (2) 审查通过了资格审查的供应商响应文件并做出评价；
- (3) 要求供应商解释或者澄清其响应文件；
- (4) 编写评审报告；
- (5) 告知采购人、采购代理机构在评审过程中发现的供应商的违法违规行

21.3 磋商小组义务

- (1) 遵纪客观、公正、审慎的原则；
- (2) 根据磋商文件的规定评审程序、评审方法和评审标准独立进行评审，对个人的评审意见承担法律责任；
- (3) 参与评审报告的起草；
- (4) 配合采购人、采购代理机构答复供应商提出的质疑；

21.4 确认磋商文件：磋商小组对磋商文件进行审阅，无修改进行签字确认，有修改，修改内容经采购人确认后，磋商小组以书面形式通知所有供应商。

22. 磋商小组成员有下列情形之一的，应当回避：

- 22.1 参加采购活动前3年内与供应商存在劳动关系；
- 22.2 参加采购活动前3年内担任供应商的董事、监事；
- 22.3 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；
- 22.4 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；
- 22.5 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。

23. 磋商程序

23.1 磋商会议

(1) 在磋商文件规定的时间和地点，由采购代理机构组织磋商工作，供应商须委派代表参加，签名以证明其出席。

(2) 各供应商或其推荐的代表与采购监督人共同检查响应文件的密封情况，经检查无误后，签字确认。

(3) 采购代理机构工作人员按照顺序，将各供应商首次响应文件的份数等内容公布，无异议后，由供应商法定代表人（或授权代表人）和监督人签字确认。

23.2 响应文件评审

23.2.1 响应文件的资格性审查。参考《政府采购法》第二十二条和磋商文件的规定，采购人或采购代理机构负责对响应文件中的资格证明文件、信用查询记录等进行审查，以确认供应商具备相应资格。资格性审查出现下列情况者（但不限于），按无效文件处理：

(1) 供应商不符合《中华人民共和国政府采购法》第二十二条的规定和特定资格条件要求的。

(2) 供应商没有经过正常渠道领取磋商文件或供应商的名称与获取磋商文件单位的名称不符。

(3) 磋商响应文件中未提交法定代表人授权书（法定代表人直接参加磋商未按要求提交其有效身份证）或授权书的合法性或有效性不符合磋商文件规定。

23.2.2 磋商响应文件有效性、完整性和响应程度审查：磋商小组负责对通过资格审查的响应文件的有效性、完整性和响应性进行审查，以确定是否满足磋商文件要求，出现下列情况者（但不限于），按无效文件处理。

(1) 供应商未按磋商文件要求加盖单位公章。

(2) 磋商响应文件未按磋商文件要求进行法定代表人或其授权代表签字。

(3) 响应文件中对合同草案条款附加了采购人难以接受的条件。

(4) 磋商内容出现漏项或数量与要求不符，出现重大负偏差。

(5) 响应报价与市场价偏离较大，低于成本，形成不正当竞争。

(6) 磋商首次报价超过最高限价或采购预算。

(7) 磋商保证金未按磋商文件要求缴纳。

23.3 磋商

23.3.1 磋商小组集中与各供应商分别进行磋商，并给所有参加磋商供应商平等的磋商机会。

23.3.2 磋商小组在对响应文件的有效性、完整性和响应程度进行审核时，以**书面形式**要求供应商对响应文件中含义不明确、同类问题表述不一致、或者明显文字和计算错误的内容在约定时间内做出必要的澄清、说明或更正。供应商澄清、说明或者更正应当由法定代表人或者授权代表签字或者加盖公章。澄清、说明或者更正不得超出响应范围，或者改变响应文件的实质性内容。

23.3.3 磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，需经采购人代表确认，并成为磋商文件的有效组成部分。

23.3.4 如出现下述情形之一的，视为供应商主动退出磋商，其响应将被拒绝：

(1) 供应商未按要求确认磋商小组确定的本项目最终技术需求的；

(2) 最后报价未实质性响应磋商小组确定的本项目最终技术需求的，或附有采购人无法接受的条件。

23.4 最后报价

23.4.1 磋商结束后，磋商小组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少于3家。最后报价是供应商响应文件的有效组成部分。

23.4.2 最后报价应按报价的格式内容填写，并且同时提交最后响应报价表、最后报价明细表。各供应商在提交响应文件时，应对最后报价加盖供应商红色公章，且由法定代表人（或授权代表人）签字。

六、确定成交单位、授予合同

25. 确定成交单位

25.1 磋商小组根据评审方法的规定对供应商进行评审排序，推荐 1-3 名成交候选人，作为评审结果。评审结果由全体磋商小组成员签字确认。

25.2 采购人根据磋商报告中推荐的成交候选人排列顺序，确定成交供应商。

25.3 成交供应商确定之后，成交结果将在陕西采购与招标网发布公告。

26. 合同

26.1 采购人在确定中标 25 日内，按照竞争性磋商文件和成交供应商竞争性磋商响应文件（包括评审中形成的澄清文件）的约定，与成交供应商签订书面合同。

27. 询问与质疑

27.1 供应商对政府采购活动事项有疑问的，可以向采购人提出询问。

27.2 供应商认为采购文件、采购过程和中标、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七个工作日内，以书面形式向采购人提出质疑。

27.3 质疑供应商在法定质疑期内须一次性提出针对同一采购程序环节的质疑。

27.4 供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- (1) 供应商的姓名或者名称、地址、邮编、联系人及联系电话；
- (2) 质疑项目的名称、编号；
- (3) 具体、明确的质疑事项和与质疑事项相关的请求；
- (4) 事实依据；
- (5) 必要的法律依据；
- (6) 提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织

的，应当由法定代表人或负责人签字或盖章，同时其授权代表签字，并加盖公章。

27.5 符合要求的质疑，采购代理机构将予以受理并答复。

联系人：李萍、王亚宁，联系电话：029-85235014

27.6 供应商进行虚假和恶意质疑的，采购代理机构将提供相关资料报监管机构，按其情况进行相应处理。

28. 履约保证金：无

29. 代理服务费：

29.1 成交供应商在领取成交通知书前，须向采购代理机构支付成交服务费，服务费由采购人与采购代理机构约定：参照国家《招标代理服务收费管理暂行办法》（计价格[2002]1980号）标准下浮20%计取，由中标人支付。

29.2 成交单位的代理服务费交纳信息

银行账户名：陕西省采购招标有限责任公司

开户银行：中国光大银行西安友谊路支行

账 号：78560188000095264

联系人：张婕 联系电话：029-85263975

30. 其他情况

30.1 成交供应商确定后，成交供应商无正当理由拖延或拒签合同的，或未能按照规定的提供履约担保，采购人有权取消其成交资格，并按评审顺序重新确定成交供应商。

第三章 评审办法和标准

1. 评审方法

本次评审采用综合评分法。磋商小组对满足磋商文件实质性要求的响应文件，按照本章第2条规定的评审标准进行打分，并按得分由高到低顺序推荐成交候选人，或根据采购人授权直接确定成交供应商。综合评分相等时，按照最后报价由低到高的顺序推荐；报价也相等的，按技术指标优劣顺序排列。

2. 评审标准

2.1 资格审查和符合性评审标准：见附表一和附表二。

2.2 分值构成：总分100分，其中

2.3 商务和技术评审标准

2.3.1 商务部分评分标准：见附表三

2.3.2 技术部分评分标准：见附表四

2.3.3 报价评分标准：见附表五

(1) 若项目未专门面向中小企业采购，对小微型企业、监狱企业、残疾人福利性单位产品的价格给予(服务10%)的扣除，用扣除后的价格参与评审。若项目专门面向中小企业采购，则不再进行价格扣除。

①根据《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)、《政府采购促进中小企业发展管理办法》(财库〔2020〕46号)，中小企业应出具《中小企业声明函》，符合工信部联企业〔2011〕300号文件规定；监狱和戒毒企业应符合《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》(财库〔2014〕68号)，并提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明；残疾人福利性单位应符合《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》(财库〔2017〕141号)文件规定，并提供《残疾人福利性单位声明函》。

②对于同时属于小微企业、监狱企业或残疾人福利性单位的，不重复进行价格扣除。

(2) 供应商提供服务所伴随产品为节能、环境标志产品，符合采购文件要求的，可优先采购，价格扣除百分比计算公式为：节能、环境标志产品清单中的产品价格占响应总价的**百分比×5%**，用扣除后的价格参与评审。

①根据《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）、《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）、环境标志产品根据《环境标志产品政府采购实施的意见》（财库〔2006〕90号）的规定，节能、环境标志产品依据品目清单和认证证书实施政府采购优先采购和强制采购。

②以在有效期之内的，国家确定的认证机构出具的节能产品、环境标志产品认证证书为依据，复印件须加盖供应商公章，否则不予扣除。

③供应商在响应文件中所响应产品为节能、环境标志品目清单中的产品，在谈判报价时必须对此类产品单独分项报价，未提供节能、环境标志产品计分明细表不予扣除。

④若节能、环境标志清单内的产品仅是构成响应产品的部件、组件或零件的，则该产品不享受鼓励优惠政策。

⑤同一包内的节能、环境标志产品部分计分只对属于清单内的非强制类产品进行计分，强制类产品不给予扣除。

⑥节能、环境标志产品不重复扣除。

(3) 评审基准价。有效响应文件中的最后报价并按本款(1)和(2)进行调整的最低报价为评审基准价。

(4) 供应商报价（按本款(1)和(2)进行调整后价格）得分=（评审基准价 / 最后报价）×价格分分值。

2.3.4 响应文件出现下列情况之一者，磋商小组在评审过程中按以下原则修正：

- (1) 大写金额与小写金额不一致的，以大写金额为准；
- (2) 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；
- (3) 单价金额小数点有明显错位的，应以总价为准，并修改单价；
- (4) 对不同文字文本响应文件的解释发生异议的，以中文文本为准；
- (5) 文字与图表不一致的，以文字为准；
- (6) 正本与副本不一致的，以正本为准；
- (7) 响应文件的文字叙述与制造厂商的产品样本/检测报告不符时，以产品样本/检测报告为准。

3. 评审程序

3.1 资格审查及符合性审查

3.1.1 采购人或采购代理机构按附表一所列审查标准对供应商资格进行审查，以确定供应商是否具备磋商资格。

3.1.2 磋商小组对符合资格要求的响应文件按附表二进行符合性审查，以确定其是否满足磋商文件的实质性要求（见本章内的符合性审查表）。

3.1.3 磋商小组在符合性审查时，可以要求供应商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作出必要的澄清、说明或更正。供应商的澄清、说明或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。

磋商小组不接受供应商主动提出的澄清、说明或补正。

供应商的书面澄清、说明和补正属于响应文件的组成部分。

磋商小组对供应商提交的澄清、说明或补正有疑问的，可以要求供应商进一步澄清、说明或补正，直至满足评审小组的要求。

3.1.4 不具备磋商文件要求的资格或未通过符合性审查的供应商，不参与磋商，由磋商小组告知该供应商。

3.1.5 通过资格审查和符合性审查的合格供应商不足 3 家的，不再进行评审和磋商。

3.2 磋商

3.2.1 按“供应商须知”第五条规定，由磋商小组与供应商进行磋商。

3.2.2 磋商过程中，磋商小组可以根据与供应商的磋商情况，在不违反相关法律法规、强制性标准、规范情况下，并经采购人代表同意后，对磋商文件的技术标准及服务要求、拟签订合同的部分条款进行变动。变动内容是磋商文件的有效组成部分，磋商小组以书面形式通知所有参加磋商的供应商。

3.2.3 磋商结束后，磋商小组可以要求所有继续参加磋商的供应商在规定时间内提交最后报价函，提交最后报价函的供应商不得少于3家。

3.3 评审

3.3.1 比较与评价

磋商小组按本章第2.3款[商务和技术评审标准]对供应商提交的响应文件（包括最后报价函）进行商务和技术评估，综合比较与评价。

磋商小组认为供应商的报价明显低于其他参与最后报价的供应商的报价或明显低于采购预算时，有可能影响产品质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，并提交相关证明材料；供应商不能证明其报价合理性的，磋商小组应当将其作为无效处理。

3.3.2 磋商小组按本章第2.3款规定的量化因素和分值进行打分，并计算出综合评估得分。

3.3.3 评分分值计算保留小数点后两位，小数点后第三位“四舍五入”。

3.4 评审结果

3.4.1 除第二章“供应商须知”前附表授权直接确定成交供应商外，磋商小组按照得分由高到低的顺序推荐3名成交候选人。

3.4.2 磋商小组完成评审后，应当向采购人提交书面评审报告。

附表一 资格审查表

序号	审查要素	审查标准	审查结果
1	法人或者其他组织、自然人的营业执照等证明文件	<p>(1) 供应商是企业（包括合伙企业）的，应提供其在市场监督管理部门注册的有效“营业执照”的复印件；</p> <p>(2) 供应商是事业单位的，应提供其有效的“事业单位法人证书”复印件；</p> <p>(3) 供应商是非企业专业服务机构的，应提供其有效的“执业许可证”复印件；</p> <p>(4) 供应商是民办非企业单位的，应提供其有效的登记证书复印件；</p> <p>(5) 供应商是个体工商户的，应提供其有效的“营业执照”复印件；</p> <p>(6) 供应商是自然人的，应提供其有效的自然人身份证明复印件。</p>	
2	财务状况报告：提供(1) 或提供(2)	<p>(1) 提供递交磋商响应文件截止之日前两年内（2023或2024年度）任意一个年度经审计的财务报告，应满足以下要求：</p> <p>① 供应商是企业的，财务报告是指经会计师事务所审计的上述指定年度整个会计年度财务报表（须提供会计师事务所出具的审计报告复印件），复印件至少须包括报告正文、资产负债表、现金流量表、利润表、附注和会计师事务所营业执照，报告正文应当有会计师事务所公章和2名注册会计师的签字及盖章。审计报告应当经过注册会计师行业统一监管平台备案赋码。</p> <p>② 供应商适用《事业单位会计准则》的，财务报告是指上述指定年度整个会计年度财务报表（不要求必须是经审计的），复印件至少须包括资产负债表、收入支出表（或收入费用表）、财政补助收入支出表。</p> <p>③ 供应商适用《政府会计准则》的，财务报告是指上述指定年度整个会计年度财务报表（不要求必须是经审计的），复印件至少须包括资产负债表、收入费用表。</p> <p>④ 供应商适用《民间非营利组织会计制度》的，财务报告是指上述指定年度整个会计年度财务报表（不要求必须是经审计的），复印件至少须包括资产负债表、业务活动表、现金流量表。</p> <p>⑤ 供应商是上述四种情况以外情况的，按照其依法适用的会计制度、财务规则或会计准则提供财务报表复印件（不要求必须是经审计的）。</p>	
		<p>(2) 提供资信证明原件或复印件，应满足以下要求：</p> <p>① 资信证明须为递交磋商响应文件截止时间前三个月内由供应商基本账户开户银行出具。</p> <p>② 无论开具银行是否标明“复印无效”，供应商提供的复印件在本次投标中予以认可（即不因“复印无效”字样而认定资信证明复印件无效）。</p> <p>③ 银行出具的存款证明不能替代银行资信证明。</p>	
3	依法缴纳税收的相关材料	<p>(1) 供应商应提供投标截止时间前近6个月中任何1个月缴税凭证，时间以税款所属时期为准（银行出具的缴税凭证或税务机关出具的证明的复印件，并加盖本单位公章）。</p>	

序号	审查要素	审查标准	审查结果
		<p>(2) 缴纳凭证复印件须清晰可辨,并能显示出供应商名称和所缴纳税种种类,单位代扣代缴的个人所得税不能作为单位纳税的凭证。</p> <p>(3) 依法免税的供应商,应提供相应文件证明其依法免税。</p>	
4	依法缴纳社会保障资金的相关材料	<p>(1) 供应商应提供投标截止时间前近6个月中至少1个月的缴纳社会保险的凭据(专用收据或社会保险缴纳清单),并加盖本单位公章。</p> <p>(2) 凭证复印件须清晰可辨,并能显示出供应商名称和所缴纳的社保的种类。</p> <p>(3) 依法不需要缴纳社会保障资金的,应提供相应文件说明其依法不需要缴纳的证明材料复印件,并加盖本单位公章。</p>	
5	具备履行合同所必需的设备 and 专业技术能力的证明材料	按照资格证明文件附件 6-5 格式作出相关承诺。	
6	参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明	按照资格证明文件附件 6-6 格式作出相关承诺。	
7	联合体协议(联合体投标时适用)	如为联合体投标,需提交联合体协议,同时联合体各方均需提供以上证明文件。	
8	特定资格要求	<p>8-1 供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为”记录名单;不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。</p> <p>(以采购代理机构于递交磋商响应文件截止时间当天进行资格审查时在“信用中国”网站(www.creditchina.gov.cn)及中国政府采购网(www.ccgp.gov.cn)查询结果为准)。</p>	
		<p>8-2 法定代表人/单位负责人身份证明书、授权委托书及授权代表在本单位缴纳养老保险证明</p> <p>(1) 法定代表人或单位负责人投标的,应提供法定代表人或单位负责人身份证明;</p> <p>(2) 授权代表投标的,应提供法定代表人或单位负责人身份证明、授权委托书及授权代表在本单位缴纳养老保险证明。</p>	
		<p>8-3 供应商须具有《网络安全等级测评与检测评估机构服务认证证书》;</p> <p>供应商需提供证书复印件并加盖公章。</p>	
		<p>8-5-1 单位负责人为同一人或者存在直接控股、管理关系的不同供应商,不得参加同一合同项下的政府采购活动</p> <p>按照资格证明文件附件 6-7 格式做出说明</p>	
		8-5-2 为本项目提供整体设计、规范编制或者项目管理、	

序号	审查要素	审查标准	审查结果
		监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动 按照资格证明文件附件 6-8 格式做出声明。	
		8-6 需向采购代理机构获取招标文件，未向采购代理机构获取招标文件的供应商均无资格参加投标。	
9	法律、行政法规规定的其他条件	不存在违反法律法规的情况	
审查结论		通过/不通过	
不通过原因说明			

注：符合要求用“√”表示，不符合用“×”表示。有一项不符合要求，结论为不合格。

附表二 符合性审查表

序号	评审项目	评审结论 (√/×)
1	供应商未按磋商文件要求加盖单位公章。	
2	磋商响应文件未按磋商文件要求进行法定代表人或其授权代表签字。	
3	响应文件中对合同草案条款附加了采购人难以接受的条件。	
4	磋商内容出现漏项或数量与要求不符，出现重大负偏差。	
5	响应报价与市场价偏离较大，低于成本，形成不正当竞争。	
6	磋商首次报价超过最高限价或采购预算。	
7	磋商保证金未按磋商文件要求缴纳	
结论（通过或未通过）		

注：1、符合磋商文件要求用“√”表示，不符合用“×”表示。有一项不符合要求，结论为不合格。

2、有下列情形之一的，视为供应商相互串通：

- (1) 不同供应商的响应文件由同一单位或者个人编制；
- (2) 不同供应商委托同一单位或者个人办理参与磋商事宜；
- (3) 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；
- (4) 不同供应商的响应文件异常一致或者报价呈规律性差异；
- (5) 不同供应商的响应文件相互混装；
- (6) 不同供应商的磋商保证金从同一单位或者个人的账户转出。

3、有下列情形之一的，属于提供虚假材料谋取成交的行为：

- (1) 使用伪造、变造的许可证件；
- (2) 提供虚假的财务状况或者业绩；
- (3) 提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；
- (4) 提供虚假的信用状况；
- (5) 其他弄虚作假的行为。

附表三 评审因素及分值分配表
(满分 100 分)

项别	分值	评审要素
报价得分	10	<p>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终报价最低的响应报价为基准价，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 / 最终磋商报价）×10 注：（小微企业、监狱企业或残疾人福利性单位用投标报价扣除后的价格参加评审。）</p>
业绩	10	<p>供应商提供 2024 年 1 月至今已完成的类似项目业绩，每提供 1 个得 1 分，最高 10 分。 注：业绩资料以合同为依据，提供合同首页、关键页和签字盖章页并加盖单位公章，其他情况不得分。</p>
服务方案及措施 评审	20	<p>供应商根据国家相关标准并结合本项目实际需求，提供完整的等级保护测评服务方案，内容包括定级备案、系统调研、初测评、差距测评、复测评等内容，并对测评流程具有详细说明。 根据提供的服务方案内容进行赋分： 1. 内容完整、详细、完整度高得 20 分； 2. 内容基本完整、基本包含、有一定的完成度得 15 分； 3. 内容不完整、完成度不高得 10 分； 4. 未提供的不得分。</p>
	10	<p>供应商针对本项目的服务提供明确的过程中的风险防范措施和保密措施，并明确保密责任与赔偿承诺。 根据提供的内容进行赋分： 1. 内容完整、详细、完整度高得 10 分； 2. 内容基本完整、基本包含、有一定的完成度得 5 分； 3. 内容不完整、完成度不高得 3 分； 4. 未提供的不得分。</p>

	10	<p>供应商针对本项目具有严格的项目质量管控措施，过程控制及监控手段，能保证技术人员按照相应的操作指南规范实施测评。</p> <p>根据提供的内容进行赋分：</p> <ol style="list-style-type: none"> 1. 内容完整、详细、完整度高得 10 分； 2. 内容基本完整、基本包含、有一定的完成度得 5 分； 3. 内容不完整、完成度不高得 3 分； 4. 未提供的不得分。
	7	<p>供应商针对项目组成员工作分配及项目实施进度具有科学合理安排，按照方案响应程度，成员工作分配科学，进度安排科学紧凑。</p> <p>根据提供的内容进行赋分：</p> <ol style="list-style-type: none"> 1. 内容完整、详细、完整度高得 7 分； 2. 内容基本完整、基本包含、有一定的完成度得 5 分； 3. 内容不完整、完成度不高得 3 分； 4. 未提供的不得分。
团队人员技术能力	5	<p>供应商针对本项目的测评团队中至少包含 2 名高级信息安全等级测评师证书，2 名中级信息安全等级测评师证书，满足条件得 1 分；在此基础上每多提供一个高级信息安全等级测评师证书得 2 分，最多得 5 分。</p> <p>注：以近三个月社保缴纳证明及全国网络安全等级保护网查询结果为准。</p>
	5	<p>供应商针对本项目提供的项目经理，在高级信息安全等级测评师证书基础上具备高级网络信息安全工程师证书、项目经理-PMP 证书、工业和信息化人才专业知识测评证书、网络安全架构师（高级）证书，每提供一个证书得 2 分，本项最多得 5 分。</p> <p>注：以证书复印件及近三个月社保缴纳证明为准。</p>
	4	<p>测评组组长具有中级信息安全等级测评师证书，同时具备高级信息系统项目管理师证书或 ITIL 证书或 CISP-PTE 证书，每提供一个证书得 2 分，本项最多得 4 分。</p> <p>注：以证书复印件及近三个月社保缴纳证明为准。</p>

合理化建议	5	<p>供应商针对服务实施过程中的关键性工作，重点、难点工作等可能影响项目实施进度的情况提出的合理化建议及解决方案。</p> <p>根据提供的内容进行赋分：</p> <ol style="list-style-type: none"> 1. 内容完整、详细、完整度高得 5 分； 2. 内容基本完整、基本包含、有一定的完成度得 3 分； 3. 内容不完整、完成度不高得 1 分； 4. 未提供的不得分。
售后服务	7	<p>为保障测评项目结束后的网络安全，供应商须提供完善的售后服务，包括应急响应服务、电话支持服务、配合检查服务、安全咨询服务、安全培训服务内容，能提供以上服务并做出相应说明，服务内容完善并有详细的说明。</p> <p>根据提供的内容进行赋分：</p> <ol style="list-style-type: none"> 1. 内容完整、详细、完整度高得 7 分； 2. 内容基本完整、基本包含、有一定的完成度得 5 分； 3. 内容不完整、完成度不高得 3 分； 4. 未提供的不得分。
培训计划	7	<p>为保证采购人的技术人员对设备的日常运维能力，供应商需提供完整、可行的培训计划，包括但不限于培训体系、培训目标、培训课程等内容。</p> <p>根据提供的内容进行赋分：</p> <ol style="list-style-type: none"> 1. 内容完整、详细、完整度高得 7 分； 2. 内容基本完整、基本包含、有一定的完成度得 5 分； 3. 内容不完整、完成度不高得 3 分； 4. 未提供的不得分。
总分	100 分	

第四章 拟签订的合同文本

甲方（采购人）：

乙方（成交供应商）：

陕西省结核病防治院网络安全等级保护测评项目（项目编号：SCZD2025-CS-2164/001），由陕西华采招标有限公司组织采购活动，_____（以下简称“甲方”）确定_____（以下简称“乙方”）为该项目的成交供应商。

依据《中华人民共和国民法典》和《中华人民共和国政府采购法》之规定，经双方在平等、自愿、互利的基础上，签订本合同，共同信守。

一、委托工作内容：_____

1. 标的一：医院信息系统,实验室信息系统,医院运营管理信息系统 占50%中标价；
2. 标的二：集成平台与数据中心 占25%中标价；
3. 标的三：综合医学影像管理与辅助诊断系统 占25%中标价。

二、交付内容：

1. 《信息系统安全等级保护定级备案证明》；
2. 《信息系统安全等级保护项目计划书》
3. 《信息系统安全等级保护测评方案》（每系统1份）
4. 《信息系统整改建议书》；
5. 《信息系统安全等级保护测评报告》（每系统1份）
6. 《信息系统安全渗透测试报告》（1份）

三、合同价款

（一）合同总价款为人民币（大写）_____（¥_____）。

（二）合同价款包括但不限于人工费、管理费、利润、风险等以及国家按现行税率征收的一切税费。

（三）合同价款一次性包死，不受市场价格变化因素的影响。

四、款项结算

1. 合同签订后，乙方入场服务。标的一服务经验收合格，乙方提供标的一全额发票，甲方收到发票后30日内，支付合同标的一合同金额。

2. 合同签订后，乙方入场服务。标的二服务经验收合格，乙方提供标的二全额发票，甲方收到发票后30日内，支付合同标的二合同金额。

3. 合同签订后，针对标的三服务内容，乙方入场时间具体以院方通知为准，乙方接到通知后，入场服务。标的三服务经验收合格，乙方提供标的三全额发票，甲方收到发票后30日内，支付合同标的三合同金额。

(二) 支付方式：银行转账。

(三) 结算方式：乙方在每次接受甲方付款前，开具等额发票给甲方。

五、服务期限及服务地点

(一) 服务期限：自各标的提供服务后一年内。

(二) 服务地点：采购人指定地点。

六、双方的权利和义务

(一) 甲方的权利与义务

1. 甲方负责配合本次项目服务工作。

2. 甲方应按本合同的约定向乙方支付合同价款。

3. 甲方根据需要对乙方提供的服务方案进行审核，提供建议及意见，确定最终实施的服务方案，以便乙方遵照执行。

4. 甲方有权对乙方的工作进行监督和考核。

(二) 乙方的权利与义务

1. 乙方应保护甲方提供的相关资料。未经甲方同意不得擅自修改、复制或向第三人转让或用于本合同外的项目，如发生以上情况，乙方应负法律责任，甲方有权向乙方提出索赔。

2. 乙方应保证提供的相关服务达到要求的质量和标准，并自觉接受甲方的监督。

3. 乙方保证安排的相关人员需按照指定时间到达指定地点进行服务，乙方在服务期间内不得迟到早退，如有特殊情况，必须事先通知并征得甲方同意。

4. 乙方在服务期间发布的任何涉及有关甲方的相关信息，需经甲方确认无误后方可发布，乙方在工作过程中接触到的与项目有关的资料、数据文件和信息等，负有保密的义务，未经甲方书面同意不得以任何方式向任何第三方提供或泄露。

5. 乙方应提供一年的售后服务工作，包括应急响应、安全监测、配合检查、电话支持、安全咨询、安全培训、制度建设、安全巡检、整改建议等服务在内的安全维保服务。具体服务内容如下：

(1)、应急响应服务

针对本次项目，服务方提供7x24h的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话10分钟内响应，如远程无法处理应在2小时内到达现场，提供服务。对采购人信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析。

(2)、配合检查服务

服务方免费协助医院响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助采购人准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

(3)、安全咨询服务

服务方为采购人免费提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全面配合采购人做好业务系统全保障工作。

(4)、安全培训服务

服务方为采购人安排计算机网络安全相关专家，开展网络安全培训，内容包含但不限于网络安全事件预警通报信息、网络安全法律、行政法规、主机安全、应用安全、网络安全、数据库安全等，提升全员网络安全防范意识和法律意识以及安全能力；在网络安全周期间，配合采购人开展网络安全宣传活动。

(5)、安全巡检服务

服务方为采购人提供不低于两次/年安全巡检服务，包括但不限于对网络设备、安全设备、服务器、终端机器以及应用服务等日志分析、版本升级、漏洞扫描以及针对linux、windows操作系统的系统漏洞升级等。

6、乙方有权要求甲方按约定支付技术服务报酬。

七、服务质量保证

(一) 乙方需派一名项目负责人，直接与甲方沟通，项目负责人接收甲方提出的问题与要求，并及时反馈给工作组，解决在项目实施过程中遇到的问题。

(二) 项目在实施过程中会出现不可预料的需求变更，乙方需积极配合甲方的需求变更，并按照变更后的需求继续进行方案实施。

(三) 乙方需建立高效的管理团队，项目团队组成合理。

(四) 乙方需设有详细的技术资料档案和服务档案，在项目完成后提交所有实施方案流程及说明文档。

八、知识产权

(一) 本项目所涉及到的所有成果的知识产权归甲方所有。

(二) 乙方无论出于任何目的如在其他地方使用该成果，必须经甲方同意方可使用。否则，甲方有权要求终止涉及到该项目知识产权的任何使用活动并保留追究卖方相应的法律责任的权利。

(三) 乙方为执行本合同而提供的技术资料使用权归甲方所有。

九、验收

(一) 验收程序：

1. 供应商向采购人提出验收申请，采购人接到供应商验收申请后组织验收专家组，按照政府采购合同约定的技术、服务、安全标准组织对供应商每一项技术、服务、安全标准的履约情况进行验收，验收合格后，出具项目验收单。

2. 验收结果作为付款依据，供应商向采购人提交服务过程中的所有资料，以便采购人日后管理和维护。

3. 采购人应当在供应商提出验收申请之日起15个工作日内完成验收。

(二) 验收依据:

1. 本合同及附加文本。
2. 磋商文件、成交供应商的响应文件及澄清（承诺）函。
3. 国家相应的标准、规范。

十、保密规定

甲、乙双方应永久恪守因签署或履行本合同而获知的对方秘密信息及其它秘密资料。任何一方如将获知的对方秘密信息泄露给第三方，应赔偿因泄密而给对方造成的一切损失并承担相应的法律责任（包括刑事责任）。

十一、其它事项

- (一) 乙方不得将项目转让、分包给其它单位或个人。
- (二) 乙方的响应文件和承诺等内容将列入合同。

十二、违约责任

- (一) 按《中华人民共和国民法典》中的相关条款执行。
- (二) 未按合同要求提供的设备质量不能满足合同技术要求，采购人有权终止合同并对供应商的违约行为进行追究。
- (三) 乙方不能按期完成工作任务，须按甲方已支付金额的双倍返还于甲方，作为赔偿。如因甲方原因导致工作任务不能按计划完成，乙方不用承担赔偿责任。

十三、合同争议解决的方式

本合同在履行过程中发生的争议，由甲、乙双方当事人协商解决，协商不成的按下列第2种方式解决：

- (一) 提交甲方所在地仲裁委员会仲裁。
- (二) 依法向甲方所在地人民法院起诉。

十四、合同解除的方式

未经甲方书面同意，乙方不得擅自解除合同。发生下列情形之一的，甲方有权单方解除合同，并要求乙方承担相应违约责任：

- (1) 乙方未按照合同约定时间完成服务工作，迟延 天仍未完成的。
- (2) 乙方的服务不符合合同约定的进度，或者工作内容不符合合同约定的，经甲方催促后3天内仍不予纠正的。
- (3) 乙方服务质量经两次验收仍不能通过甲方或第三方验收的。
- (4) 合同约定的乙方负责人及技术人员未实际参与本项目工作，或乙方擅自更换上述人员的，经甲方通知后3天内仍未纠正的。
- (5) 乙方擅自将项目全部或部分内容转委托的。
- (6) 乙方丧失履约能力的或者明确表示不能完成本合同约定的技术服务工作的。
- (7) 合同约定的其他解除情形。

十五、合同变更的方式

本合同的任何修改、补充或变更，均须双方协商一致，并以书面形式订立，由双方法定代表人或授权代表签字并加盖公章（或合同专用章）后方可生效。任何口头承诺或陈述均不对本合同产生变更效力。

十六、合同生效

（一）本合同须经甲、乙双方的法定代表人（授权代理人）在合同书上签字并加盖本单位公章后正式生效。

（二）合同生效后，甲、乙双方须严格执行本合同条款的规定，全面履行合同，违者按《中华人民共和国民法典》的有关规定承担相应责任。

（三）本合同一式___份，甲乙双方各执___份。

（四）本合同如有未尽事宜，甲、乙双方协商解决。

甲 方

乙 方

（盖章）

（盖章）

地址：

地址：

法定代表人：

法定代表人：

被授权代表：

被授权代表：

电话：

电话：

传真：

传真：

开户银行：

开户银行：

日期：

日期：

第六章 采购内容及要求

根据国家《信息安全等级保护管理办法》（公通字[2007]43号）、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）、《陕西省信息安全等级保护安全建设整改工作指导意见》（陕等保办20112号）等相关文件要求，对“医院信息系统、实验室信息系统、医院运营管理信息系统、集成平台及数据中心以及综合医学影像管理与辅助诊断系统”信息系统实施网络安全等级保护测评工作。

一、项目服务内容

序号	系统名称	系统级别
1	医院信息系统	三级
2	实验室信息系统	三级
3	医院运营管理信息系统	三级
4	集成平台及数据中心	三级
5	综合医学影像管理与辅助诊断系统	三级

标的一：医院信息系统；实验室信息系统；医院运营管理信息系统三级等保的复评；

标的二：集成平台及数据中心三级等保的测评；

标的三：综合医学影像管理与辅助诊断系统；

1. 系统调研：在系统相关人员的协助下，对上述信息系统进行调研和梳理，了解系统当前信息系统资产现状。
2. 现场测评：根据国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果。

3. 分析整改：根据前述工作内容，分析信息系统安全情况与等级保护基本要求的差距，提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合采购单位安全整改工作。

4. 结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评，提供安全等级符合性测评服务，出具相关系统测评报告。

5. 配合验收：整理项目过程中所有相关的过程文档，提交系统相关人员。

二、其他要求

1. 测评人员要求：本项目的测评人员需具有 2 年或 2 年以上测评工作经验，项目经理和质量负责人必须具备丰富的安全服务经验及相关资质认证，并提供人员管理及配备方案，并确保人员稳定。如需更换测评人员，须由采购单位同意。

2. 人员配备：投标方参与此项目不少于 8 人，现场测评人员不得少于 6 人，其中至少包含 2 名高级测评师，4 名中级测评师。供应商必须为本项目成立本地化等级保护测评小组，由测评小组组长统一负责，测评小组组长具有一定的技术及管理知识和经验，能容易地与客户沟通，能很好的执行与完成测评工作，并根据适当情况增加测评人员。

3. 供应商应按等级保护测评要求制定测评过程中产生的文档，做到科学、规范、详尽、统一。

三、项目技术标准及要求

(1) 总体要求

根据国家《信息安全等级保护管理办法》(公通字[2007]43号)与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019 要求，等级测评工作须覆盖安全物理环境、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、安全运维管理等方面的内容，并根据现场实际情况完成风险分析工作，最终为完善等级保护安全防护体系提供指导依据。

第一阶段：等级保护

网络安全等级保护工作共分为五步，分别是：“定级、备案、建设整改、等级测评、监督检查”。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、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、安全运维管理十个安全类别进行安全测评。

1. 定级要求

该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020）确定系统等级。

2. 备案

信息系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。

完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

3. 等级保护测评要求

供应商在测评过程中要求按照《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 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安全等级保护测评要求》

(GB/T28448-2019)、《信息安全技术 网络安全等级保护测评过程指南》(GB/T28449-2018)等相关的标准规范开展等级测评工作,对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。测评指标如下:

等级保护技术要求

安全层面	安全控制点	测评指标
安全物理环境	物理位置选择	a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑物内;
		b) 机房场地应避免设在建筑物的高层或地下室,否则应加强防水和防潮措施。
	物理访问控制	a) 机房出入口应配置电子门禁系统,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;
		c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地;
		b) 应采取措施防止感应雷,例如设置防雷保安器或过压保护装置等。
	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;
c) 应对机房划分区域进行管理,区域和区域之间设置隔离防火措施。		
防水防潮	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;	

安全层面	安全控制点	测评指标
		c) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
	防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施；
		b) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	a) 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；
c) 应设置冗余或并行的电力电缆线路为计算机系统供电。		
电磁防护	a) 电源线和通信线缆应隔离铺设，避免互相干扰；	
	b) 应对关键设备实施电磁屏蔽。	
安全通信网络	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要；
		b) 应保证网络各个部分的带宽满足业务高峰期需要；
		c) 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；
		d) 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；
		e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a) 应采用校验技术或密码技术保证通信过程中数据的完整性；
b) 应采用密码技术保证通信过程中数据的保密性。		
可信验证	a) 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，并在应用程序的关键执行环节进行动态可信验证，在监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	边界防护	a) 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；
		b) 应能够对非授权设备私自联到内部网络的行为进行检测或限制；
		c) 应能够对内部用户非授权联到外部网络的行为进行检查或

安全层面	安全控制点	测评指标
安全层面		限制；
		d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	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；
		e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
		b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
		c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
		d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a) 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；
		b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件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、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；
		d) 应能对远程访问的用户行为、访问互联网的用户行为等单独

安全层面	安全控制点	测评指标
		进行行为审计和数据分析。
	可信验证	a) 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，并在应用程序的关键执行环节进行动态可信验证，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。
安全计算环境	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) 应启用登陆失败处理功能，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；
		d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术实现。
	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；
		e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
	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、时间、事件类型、事件是否成功及其他与审计相关的工作；
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；		
d) 应对审计进程进行保护，防止未经授权的中断。		

安全层面	安全控制点	测评指标
	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； f) 应能检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	a) 应采用免受恶意代码攻击的技术措施，或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	a) 可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，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	a) 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于数据鉴别、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于数据鉴别、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于数据鉴别、重要业务数据和重要个人信息等。
	数据备份和恢复	a) 应提供重要数据的本地数据备份与恢复功能； b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备用场地； c) 应提供重要数据处理系统的冗余，保证系统的高可用性。
	剩余信息保护	a) 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； b) 应保证存有敏感数据的存储空间被释放或重新分配前得到

安全层面	安全控制点	测评指标
		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。
	安全管理	a) 应对安全管理员进行身份鉴别，只允许通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体，客体进行统一安全标识，对主体进行授权，配置安全可信验证策略等。
	集中管控	a) 应划分特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
		b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
		c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；		
e) 应对安全策略、安全代码、补丁升级等安全事项进行集中管理；		
f) 应能对网络中发生的各类安全事件进行识别报警和分析。		
安全管理	安全策略	a) 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。
	管理制度	a) 应对安全管理活动中的各类管理内容建立安全管理制度；
		b) 应对要求管理人员或操作人员执行的日常管理操作建立操

安全层面	安全控制点	测评指标
制度		作规程；
		c) 应形成由安全策略，管理制度，操作规程，记录表单等构成安全管理制度体系。
	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	a) 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) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b) 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；
		c) 应设立系统管理员、审计管理员、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	a) 应配备一定数量的系统管理员、审计管理员、安全管理员等；
		b) 应配备专职的安全管理员，不可兼任。
	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建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
		c) 应定期审查审批事项，及时更新授权和审批的项目、审批部门和审批人等信息。
	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	a) 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；	

安全层面	安全控制点	测评指标
	查	<p>b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置和安全策略的一致性，安全管理制度的执行情况等；</p> <p>c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。</p>
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) 应对被录用人的身份、安全背景、专业资格或资质等进行审查，对其所有的技术技能进行考核；
		c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a) 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；
		b) 应办理严格的调离手续，并承诺调离后的保密义务方可离开。
	安全意识教育和培训	a) 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；
		b) 应针对不同岗位制定不同的培训计划，对安全基础知识，岗位操作规程等进行培训；
c) 应定期对不同岗位的人员进行技能考核。		
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；	
	d) 获得系统访问授权的外部人员签署保密协议，不得进行非授权操作，不得复制和泄露敏感信息。	
安全建设管理	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安全保护等级的方法和理由；
		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	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

安全层面	安全控制点	测评指标
	方案设计	<p>结果补充和调整安全措施；</p> <p>b) 应根据保护对象的安全保护等级及与其他级别对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容、并形成配套文件；</p> <p>c) 应组织相关部门和有关安全技术专家对整体安全规划及其配套文件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。</p>
	产品采购和使用	<p>a) 应确保网络安全产品采购和使用符合国家的有关规定；</p> <p>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；</p> <p>c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新产品候选名单。</p>
	自行软件开发	<p>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；</p> <p>b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；</p> <p>c) 应制定代码编写安全规范，要求开发人员参照规范编写代码；</p> <p>d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；</p> <p>e) 应保证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；</p> <p>f) 应对程序资源库的修改、更新，发布进行授权和批准，并严格进行版本控制；</p> <p>g) 应保证开发人员为专职人员，开发人员的开发活动受到控制，监视和审查。</p>
	外包软件开发	<p>a) 应在软件交付前检测其中可能存在的恶意代码；</p> <p>b) 应保证开发单位提供软件设计文档和使用指南；</p> <p>c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后面和隐蔽信道。</p>
	工程实施	<p>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；</p> <p>b) 应制定安全工程实施方案控制实施过程；</p> <p>c) 应通过第三方工程监理控制项目的实施过程。</p>

安全层面	安全控制点	测评指标
	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，安全测试报告应包含密码应用安全性安全测试内容。
	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) 应对负责系统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) 在发生重大变化或级别发生时进行等级测评；
		c) 应确保测评机构的选择符合国家相关规定。
	服务供应商管理	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；
c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务进行控制。		
安全运维管理	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) 应建立机房安全管理制度，对有关物理访问，物品带进带出和环境安全等方面的管理作出规定；
		c) 应不在重要区域接待来访人员，不随意放置包含敏感信息的纸质文件和移动介质。
	资产管理	a) 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
		b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
		c) 应对信息分类与标识方法做出规定，并对信息的使用，传输和存储等进行规范化管理。
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；	

安全层面	安全控制点	测评指标
		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，并对介质归档和查询等进行登记记录。
	设备维护管理	<p>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；</p> <p>b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，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；</p> <p>c) 信息处理设备应经过审批才能带离机房或办公地点，含有储存介质的设备带出工作环境时其重要数据应加密；</p> <p>d) 含有存储介质的设备在报废或重用前，应进行完全清除或完全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。</p>
	漏洞和风险管理	<p>a) 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；</p> <p>b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。</p>
	网络系统安全管理	<p>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；</p> <p>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；</p> <p>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作出规定；</p> <p>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；</p> <p>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、参数的设置和修改的内容；</p> <p>f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；</p> <p>g) 应严格控制变更性运维，经过审批后才可改变连接，安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步配置更新配置信息库；</p> <p>H) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删</p>

安全层面	安全控制点	测评指标
		<p>除工具中的敏感数据；</p> <p>i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；</p> <p>j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略行为。</p>
	恶意代码防范管理	<p>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；</p> <p>b) 应定期验证防范恶意代码攻击的技术措施的有效性。</p>
	配置管理	<p>a) 应记录和保存基本配置信息，包括网络拓扑结构、各类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；</p> <p>b) 应将基本信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。</p>
	密码管理	<p>a) 应遵循密码相关国家标准和行业标准；</p> <p>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。</p>
	变更管理	<p>a) 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；</p> <p>b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；</p> <p>c) 应建立终止变更并从失败的变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。</p>
	备份与恢复管理	<p>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；</p> <p>b) 应规定备份信息的备份方式、备份频度、存储介质和保存期等；</p> <p>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。</p>
	安全事件处置	<p>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；</p> <p>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；</p>

安全层面	安全控制点	测评指标
		c) 应在安全事件和响应处理过程中，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； d) 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序。
	应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件，应急组织构成，应急资源保障，事后教育和培训等内容； b) 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； c) 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； d) 应定期对原有的应急预案重新评估，修订完善。
	外包运维管理	a) 应确保外包运维供应商的选择符合国家有关规定； b) 应与选定的外包运维供应商签订相关的协议，明确约定外包运维的范围、工作内容； c) 应保证选择的外包运维供应商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力在签订的协议中明确； d) 应在与外包运维供应商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、储存要求，对 IT 基础设施中断服务的应急保障要求等。

第二阶段：渗透检测

渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机信息系统是否安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，通常该分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

第三阶段：建设整改咨询及安全加固（不涉及硬件）

建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；将信息系统的安全建设整改需求落

实到可操作的安全技术和管理的上，提出能够实现的技术参数或制度及其具体规范。

之后依据相关《信息系统安全建设整改建议》开展建设整改工作时，服务方将提供建设整改过程中的与建设整改相关的咨询服务。

对信息系统安全整改建议进行确认，并依照建议，协助我方进行漏洞修复，补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，然后协助我方分步实施安全整改工作。

第四阶段：售后服务

为期一年的售后服务工作中，服务方将向采购人提供包括应急响应、安全监测、配合检查、电话支持、安全咨询、安全培训、制度建设、安全巡检、整改建议等服务在内的安全维保服务。具体服务内容如下：

(1)、应急响应服务

针对本次项目，服务方提供 7x24h 的常规应急响应及灾难恢复专家服务。在接到用户故障报修电话 10 分钟内响应，如远程无法处理应在 2 小时内到达现场，提供服务。对采购人信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析。

(2)、配合检查服务

服务方免费协助医院响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助采购人准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

(3)、安全咨询服务

服务方为采购人免费提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到用户的服务请求，技术服务工程师将立即开始提供服务，帮助客户解决信息安全相关技术问题，全

面配合采购人做好业务系统全保障工作。

(4)、安全培训服务

服务方为采购人安排计算机网络安全相关专家，开展网络安全培训，内容包含但不限于网络安全事件预警通报信息、网络安全法律、行政法规、主机安全、应用安全、网络安全、数据库安全等，提升全员网络安全防范意识和法律意识以及安全能力；在网络安全周期间，配合采购人开展网络安全宣传活动。

(5)、安全巡检服务

服务方为采购人提供不低于两次/年安全巡检服务，包括但不限于对网络设备、安全设备、服务器、终端机器以及应用服务等日志分析、版本升级、漏洞扫描以及针对 linux、windows 操作系统的系统漏洞升级等。

(2)交付内容

1. 《信息系统安全等级保护定级备案证明》；
2. 《信息系统安全等级保护项目计划书》
3. 《信息系统安全等级保护测评方案》（每系统 1 份）
4. 《信息系统整改建议书》；
5. 《信息系统安全等级保护测评报告》（每系统 1 份）
6. 《信息系统安全渗透测试报告》（1 份）

第七章 磋商响应文件格式

正本/副本

项目编号：

*******项目**

磋商响应文件

供应商：_____

时 间：_____

目录

具体目录内容可扩展

第一部分 身份证明文件

第二部分 资格证明文件

第三部分 磋商响应函

第四部分 磋商响应报价表

第五部分 偏离表

第六部分 响应方案说明

第一部分 身份证明文件

1、法定代表人（或单位负责人）授权书

本授权书声明：注册于（国家或地区的名称）的（供应商）的（法人代表姓名、职务）为我单位法定代表人，代表我单位授权（被授权人的姓名）为我单位的合法代理人，就（项目名称和采购项目编号）投标，以我单位名义处理一切与之有关的事务。

本授权书于_____年___月___日签字生效，特此声明。（提示：此日期应不晚于投标函签署日期）

附：授权代表姓名：_____性别：___年龄：_____

职 务：_____身份证号码：_____

通讯地址：_____

邮政编码：_____ 电话：_____

法定代表人及授权代表身份证复印件

法定代表人身份证复印件 (正反面)	授权代表身份证复印件 (正反面)
----------------------	---------------------

供应商

(公章)：

法定代表人

(签字或盖章)：

注：自然人投标的或法定代表人投标的无需提供

2、法定代表人（或单位负责人）身份证明

（采购代理机构名称）：

_____（姓名、性别、年龄、身份证号码）在我单位任_____（董事长、总经理等）职务，是我单位的法定代表人。

特此证明。

供应商（盖公章）：_____

详细通讯地址：_____

邮 政 编 码：_____

电 话：_____

注：自然人投标的仅提供身份证

3、授权代表本单位证明

(提供授权代表在本单位养老保险缴纳证明)

第二部分 资格证明文件

符合《政府采购法》第二十二条的规定供应商条件，并提供以下证明材料；

(1) 供应商合法注册的法人或其他组织的营业执照等证明文件，自然人的身份证明（格式要求见附件 6-1）；

(2) 磋商响应文件截止之日前两年(2023 或 2024 年度)内任意一个年度经审计的财务报告复印件（包括报告正文、资产负债表、现金流量表、利润表、附注和会计师事务所营业执照，报告正文应当有会计师事务所公章和 2 名注册会计师的签字及盖章。且审计报告应当经过注册会计师行业统一监管平台备案赋码。），或递交磋商响应文件截止时间前三个月内供应商基本账户开户银行出具的资信证明（格式要求见附件 6-2）；

(3) 依法缴纳税收和社会保障资金的证明材料复印件（格式见附件 6-3、6-4）

(4) 具备履行合同所必需的设备和专业技术能力的承诺原件（格式见附件 6-5）

(5) 供应商参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明原件（格式见附件 6-6）

(6) 供应商控股股东名称、控股公司的名称和存在管理、被管理关系的单位名称说明（格式见附件 6-7）

(7) 供应商是否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声明原件（格式见附件 6-8）

(8) 证明供应商符合特定资格条件的证明材料；（格式见附件 6-9）

(9) 若为小微企业或残疾人福利企业等提供声明函（格式件附件 6-10）

要求：以上资格证明文件须提供加盖供应商公章的扫描件。

6-1 供应商的企业法人营业执照副本扫描件（加盖公章）

（注：根据项目实际情况，本项内容可能要求提供“事业单位法人证书”、执业许可证、自然人身份证明等证明材料）

6-2 供应商必须拥有良好的商业信誉

供应商提供磋商响应文件截止之日前两年（2023 或 2024 年度）内任意一个年度经审计的财务报告（包括报告正文、资产负债表、现金流量表、利润表、附注和会计师事务所营业执照，报告正文应当有会计师事务所公章和 2 名注册会计师的签字及盖章。且 2022 年 10 月 1 日后出具的审计报告应当经过注册会计师行业统一监管平台备案赋码。）复印件或扫描件，所有复印件或扫描件需加盖单位公章。

或 6-2 递交磋商响应文件截止时间前三个月内供应商基本账户开户银行出具的资信证明

6-3 依法缴纳税收的证明

说明：

- 1、供应商应提供投标截止时间前近 6 个月中任何 1 个月缴税凭证，时间以税款所属时期为准（银行出具的缴税凭证或税务机关出具的证明的复印件，并加盖本单位公章）。
- 2、依法免税或无须缴纳税收的供应商，应提供相应证明文件。

6-4 社会保障资金缴纳记录

说明：

- 1、供应商应提供投标截止时间前近 6 个月中至少 1 个月的缴纳社会保险的凭据（专用收据或社会保险缴纳清单），并加盖本单位公章。
- 2、不需要缴纳社会保障资金的供应商，应提供相应文件证明其不需要缴纳社会保障资金。

6-5 具备履行合同所必需的设备和专业技术能力承诺书

陕西省采购招标有限责任公司：

我公司承诺具备履行合同所必需的设备和专业技术能力。

供应商名称（公章）： _____

法定代表人或其授权代表（签字或加盖人名章）： _____

日 期： _____年_____月_____日

6-6 供应商参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明

陕西省采购招标有限责任公司：

我公司郑重承诺在参加本项目政府采购活动前三年内，在经营活动中无重大违法记录。

特此声明。

供应商名称（公章）： _____

法定代表人或其授权代表（签字或加盖人名章）： _____

日 期： _____年_____月_____日

6-7 供应商控股股东名称、控股公司的名称和存在管理、被管理关系的单位名称说明

陕西省采购招标有限责任公司：

与我方的法定代表人（单位负责人）为同一人的企业如下：

我方的控股股东如下：

我方直接控股的企业如下：

与我方存在管理、被管理关系的单位名称如下：

供应商名称（公章）： _____

法定代表人或其授权代表（签字或加盖人名章）： _____

日 期： _____年_____月_____日

6-8 供应商是否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声明

陕西省采购招标有限责任公司：

我方 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。

供应商名称（公章）： _____

法定代表人或其授权代表（签字或加盖人名章）： _____

日 期： _____年_____月_____日

6-9 证明供应商符合特定资格条件的证明材料：详见磋商公告的特点资格要求

(1) 中小企业声明函（服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

2. （标的名称），属于（采购文件中明确的所属行业）；承建（承接）企业为（企业名称），从业人员 人，营业收入为 万元，资产总额为 万元，属于（中型企业、小型企业、微型企业）；

.....

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

（从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报）

(2) 监狱企业声明函

本单位郑重声明下列事项（按照实际情况勾选或填空）：

本单位为直接供应商，提供本单位制造的货物。

(1) 本企业（单位）_____（请填写：是、不是）监狱企业。如果是，后附省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

(2) 本企业（单位）_____（请填写：是、不是）为联合体一方，提供本企业（单位）制造的货物，由本企业（单位）承担工程、提供服务。本企业（单位）提供协议合同金额占到共同投标协议合同总金额的比例为_____。

本企业（单位）对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商（盖公章）：_____

法定代表人或委托代理人（签字或盖章）：_____

日期：_____

注：符合《关于政府采购支持监狱企业发展有关问题的通知》价格扣减条件的供应商须提交。需提供省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

(3) 残疾人福利性单位声明函

(注：符合条件的残疾人福利性单位请提供本函，不符合的不提供本函)

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商（盖公章）：_____

法定代表人或委托代理人（签字或盖章）：_____

日期：_____

地 址： _____

开户银行： _____

帐 号： _____

电 话： _____ 传 真： _____

供应商全称（公章）： _____

法定代表人或授权代表（签字或盖章）： _____

_____年_____月_____日

第四部分 磋商响应报价表

首次响应报价表

项目编号及名称	项目编号： _____ 项目名称： _____
磋商报价	人民币（大写）： _____ 整 （小写： ¥ _____ 元）
服务期限	
备注	

供应商
(公章)：

法定代表人或授权代表
(签字或盖章)

_____年 _____月 _____日

首次响应分项报价表

项目编号： _____

项目名称： _____

序号	服务内容	报价	备注
1			
2			
3			
4			
5			
6			
7			
8			
磋商报价合计： _____元			

供应商
(公章)：

法定代表人或授权代表
(签字或盖章)

_____年 _____月 _____日

第五部分 偏离表

1. 商务、合同条款偏离表

项目编号：

项目名称：

序号	磋商文件商务、合同条款	供应商响应情况	有无偏离 (有/无)	有偏离(正偏离/ 负偏离)	偏离简述
	...				

供应商（公章）： _____

法定代表人或其授权代表（签字或盖章）： _____

日期： ____年____月____日

注：1、对有偏离的条目在本表相应列中标注“正偏离”或“负偏离”，并在“偏离简述”栏中加以说明。**商务要求不得负偏离，否则视为无效文件。**

2、正偏离是指应答的条件高于磋商文件要求，负偏离是指应答的条件低于磋商文件要求，正偏离项目不作扣分处理。

3、供应商须完整填写响应表。

4、在采购人与成交供应商签订合同时，如成交供应商未在响应文件“响应表”中列出偏离说明，无论已发生或即将发生任何情形，均视为完全符合磋商文件要求，并写入合同。若成交供应商在合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作拒绝与采购人签订合同。

2. 技术偏离表

项目编号： _____

项目名称： _____

磋商文件 技术条款 要求	供应商响应 文件内容	有无偏离 (有/无)	有偏离（正偏离/ 负偏离）	偏离简述	证明材料页 码

供应商（公章）： _____

法定代表人或其授权代表（签字或盖章）： _____

日 期： _____年_____月_____日

- 注：1. 对有偏离的条目在本表相应列中标注“正偏离”或“负偏离”。并在“偏离简述”栏中加以说明。
2. 正偏离是指应答的条件高于磋商文件要求，负偏离是指应答的条件低于磋商文件要求，正偏离项目不作扣分处理。
- 3 供应商须按照用户需求书逐条完整填写响应表。
- 4 在采购人与成交供应商签订合同时，如成交供应商未在响应文件“响应表”中列出偏离说明，无论即将发生或已发生任何情形，均视为完全符合磋商文件要求，并写入合同。若成交供应商在合同签订前，以上述事项为借口而不履行合同签订手续及执行合同，则视作拒绝与采购人签订合同。

第六部分 响应方案说明

(格式自拟, 内容需符合评审办法中要求的内容要求)

附件

(最后) 磋商响应报价表

(随身携带, 单独提供, 无需装订在响应文件中)

项目编号及名称	项目编号: _____ 项目名称: _____
磋商报价	人民币(大写): _____ 整 (小写: ¥_____元)
服务期限	
备注	

供应商
(公章):

法定代表人或授权代表
(签字或盖章):

_____年 _____月 _____日

(最后) 磋商响应分项报价表

(随身携带, 单独提供, 无需装订在响应文件中)

项目编号: _____

项目名称: _____

序号	服务内容	报价	备注
1			
2			
3			
4			
5			
6			
7			
8			
磋商报价合计:			_____元

供应商
(公章):

法定代表人或授权代表
(签字或盖章)

_____年 _____月 _____日