招 标 文 件

（货物类）

采购项目名称：铜川市政务云平台安全能力提升建设项目

采购项目编号：QH-2026-ZB-TC-022

铜川市数据中心

秦汉项目管理有限公司共同编制

2026年09月22日

第一章 投标邀请

秦汉项目管理有限公司（以下简称“代理机构”）受铜川市数据中心委托，拟对铜川市政务云平台安全能力提升建设项目进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：QH-2026-ZB-TC-022

二、采购项目名称：铜川市政务云平台安全能力提升建设项目

三、招标项目简介

按照中省国产化适配迁移任务要求，为加快提升我市政务云平台安全保障能力，有效保障政务云平台和上云政务信息系统安全稳定运行，我们将新增防火墙、威胁情报网关、综合网管系统等网络安全设备和系统，续保现有入侵防御系统、远程安全评估系统等安全设备，构建政务云平台互联网区和政务外网区双区域网络边界安全防护体系；新建1套网络安全态势感知平台，配套探针和日志审计系统，实现政务云平台双区全域安全态势可视、威胁精准识别；新建政务云平台政务外网区、互联网区云安全资源池，为全市各级各部门上云政务信息系统提供主机安全、日志审计等安全组件，实现专属安全服务。通过构建一个功能完备的纵深防护体系，将极大提升政务云平台安全防护能力和预警监测能力，有力支撑全市政务信息系统迁移上云合规要求，为全市数字政府建设与经济社会高质量发展提供坚实可靠的安全保障。

四、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：

1.落实政府采购促进中小企业发展的相关政策

无

（三）本项目的特定资格要求：

采购包1：

1、主体资格：供应商应为具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

2、税收缴纳证明：提供文件递交截止日前六个月内任意1个月的纳税证明或完税证明，相关证明材料，证明资料上应有相关机构的公章或业务专用章。依法免税的投标人应提供相关文件证明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

3、社会保障资金缴纳证明：提供文件递交截止日前六个月内任意1个月的社会保障资金相关证明材料，证明资料上应有相关机构的公章或业务专用章。依法不需要缴纳社会保障资金的投标人应提供相关文件证明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

4、承诺函：提供具有履行合同所必需的设备和专业技术能力的承诺函；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

5、信誉要求：供应商不得为“信用中国”中列入失信被执行人和重大税收违法案件当事人名单的供应商，不得为“中国政府采购网” 政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商，提供截图和承诺书。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章

6、授权代表：提供法定代表人授权书（附有效的法定代表人、被授权人身份证复印件）；法定代表人直接参加投标的，只须提供法定代表人身份证明文件；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

7、无违法记录证明：供应商出具本企业参加政府采购活动前三年内经营活动中没有重大违法记录的书面声明。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

8、不接受联合体投标：提供非联合体声明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。

五、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：陕西省政府采购综合管理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：通过陕西省政府采购网（https://www.ccgp-shaanxi.gov.cn/）首页供应商用户登录陕西省政府采购综合管理平台（以下简称“政府采购平台”），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）供应商应当自行在陕西省政府采购网-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、使用政府采购平台前，应当按照要求完成供应商注册和信息完善，加入政府采购平台供应商库。

（二）供应商应当使用纳入陕西省政府采购综合管理平台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在政府采购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，可查看陕西省政府采购网-办事指南-CA及签章服务。

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）政府采购平台技术支持：

在线服务：通过陕西省政府采购网-在线服务进行咨询。

技术服务电话：029-96702。

CA及签章服务：通过陕西省政府采购网-办事指南-CA及签章服务查看CA办理流程。

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告。

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

成功获取招标文件后，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投标文件编制的，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招标文件，供应商应当重新获取招标文件；澄清或者修改后的招标文件发布日期距提交投标文件截止日期不足15日的，采购人或代理机构顺延提交投标文件的截止时间。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

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

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告。

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在陕西省政府采购网以公告形式发布

九、供应商信用融资

根据《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）和《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23 号）文件要求，为助力解决政府采购成交供应商资金不足、融资难、融资贵的问题，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陕西省政府采购网—陕西省政府采购金融服务平台（https://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/），选择符合自身情况的“政采贷”银行及其产品，凭项目中标（成交）结果、中标（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、联系方式

采购人： 铜川市数据中心

地址： 铜川市正阳路9号

邮编： 727000

联系人： 巨三建

联系电话： 0919-3183142

代理机构：秦汉项目管理有限公司

地址： 陕西省西安市雁塔区陕西省西安市曲江新区雁展路莱安中心T3栋403室

邮编： 710000

联系人： 任英沛

联系电话： 18700895616

采购监督机构：铜川市财政局政府采购管理科

联系人：郭老师

联系电话：0919-3281620

第二章 投标人须知

2.1投标人须知前附表

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1：6,881,018.00元 投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。
2	最高限价（实质性要求）	详见第三章。 投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。
3	评标方法	采购包1：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 如以联合体投标的，联合体各方均应当具备本招标文件要求的资格条件和能力。 1.两个以上供应商可以组成一个联合体，以一个供应商的身份参加采购活动。以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。 2.参加联合体的供应商均应当具备本法第二十二条规定的条件，并应当向采购人提交联合协议，载明联合体各方承担的工作和义务。联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。 3.联合体各方应当共同与采购人签订采购合同，就采购合同约定的事项对采购人承担连带责任。
5	落实节能、环保产品政策	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/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，否则作无效投标处理。 3.本项目采购的/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/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/响应报价相同的，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。
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）	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	本国产品价格扣除（若采购项目适用本国产品标准）	本项目应执行《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）及《关于贯彻落实<国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知>的意见》（财库〔2025〕30号）的要求，本项目采购包中执行本国产品价格扣除情况，具体扣除比例及规则见采购文件第五章。
8	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。 使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。 采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。 核心产品清单详见第三章。 在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。

9	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会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。投标人提交的书面说明，应当加盖投标人公章，在评标委员会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投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
10	异常低价审查	本项目应执行财政部《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）的要求，具体内容见采购文件第五章。
11	投标保证金	缴交方式：否 注：电子保函可通过陕西省政府采购金融服务平台申请办理。
12	标书费信息	免费获取
13	履约保证金（实质性要求）	采购包1：不缴纳
14	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。
15	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：参照甲方在铜川市中介服务超市选取招标代理机构发布的预算金额在项目中标结果发布后与中标(成交)供应商协商收取，项目结束后一次性付清。
16	采购结果公告	采购结果将在陕西省政府采购网予以公告。
17	中标通知书	采购结果公告发布的同时，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
18	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“陕西省政府采购网”予以公告；政府采购合同签订之日起7个工作日内，采购人将本项目采购合同通过政府采购平台进行备案。
19	进口产品	不允许
20	是否组织潜在供应商现场考察	采购包1：组织现场踏勘：否
21	特殊情况	出现下列情形之一的，采购人或者采购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废标。
22	其他说明	本采购文件所称的“以上”、“以下”、“内”、“以内”、“不少于”包括本数；所称的“不足”、“低于”、“超过”不包括本数。

2.2总则

2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由铜川市数据中心和秦汉项目管理有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由铜川市数据中心负责解释。除上述招标文件内容，其他内容由秦汉项目管理有限公司负责解释。

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。本次招标的采购人是铜川市数据中心。

二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物、工程或服务的法人、其他组织或者自然人。

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秦汉项目管理有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成资格审查小组和评审小组组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选供应商等活动。

2.3招标文件

2.3.1招标文件的构成

一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：

（一）投标邀请；

（二）投标人须知；

（三）招标项目技术、服务、商务及其他要求；

（四）资格审查；

（五）评标办法；

（六）投标文件格式；

（七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面做出实质性响应所产生的风险由投标人承担。

2.3.2招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，投标人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。更正内容可能影响投标文件编制的，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招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4投标文件

2.4.1投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标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，评标委员会将其视为无效材料。

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投标人的不利后果，由投标人承担。

2.4.2计量单位

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3投标货币

本次项目均以人民币报价。

2.4.4知识产权

一、投标人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，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。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，采购项目涉及采购标的的知识产权相关事宜由采购人结合项目实际自主确认或协商约定，具体如下：

中标供应商保证所投产品及交付成果知识产权合法有效，不侵犯任何第三方权利；本项目交付成果知识产权归采购人所有。

三、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5投标文件的组成

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

2.4.6投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子签章，投标人未在规定时间内确认的，其投标无效。

2.4.8投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9投标文件的制作、签章和加密（实质性要求）

一、投标文件应当根据招标文件进行编制，投标人应通过陕西省政府采购网-办事指南-CA及签章服务下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标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招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5开标、资格审查、评标和中标

2.5.1开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

开标/开启前30分钟内，供应商需登录项目电子化交易系统-“供应商开标大厅”-进入开标选择对应项目包组操作签到，签到完成后等待代理机构开标/开启。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人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采购系统进行投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，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。投标人对开标过程和开标记录有疑义，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投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

2.5.2查询及使用信用记录

开标结束后，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，查询投标人在投标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、重大税收违法失信主体名单、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，以一个投标人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

详见招标文件第四章。

2.5.4评标

详见招标文件第五章。

2.5.5中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在陕西省政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标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、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标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、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标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。分包供应商履行的分包项目的品牌、规格型号及技术要求等，必须与中标的品牌、规格型号及技术要求一致。

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，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人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。

2.6.2.2合同转包

一、严禁中标人将本项目转包。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、中标人转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3合同公告

采购人应当自政府采购合同签订（双方当事人均已完成盖章）之日起2个工作日内，在陕西省政府采购网公告本项目采购合同，但合同中涉及国家秘密、商业秘密的内容除外。

2.6.4合同备案

采购人自政府采购合同签订（双方当事人均已完成盖章）之日起7个工作日内，将本项目采购合同报同级财政部门备案。

2.6.5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，可以与中标人协商签订补充合同，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。

2.6.6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。

2.6.7履约验收方案

采购包1:

符合招标文件、投标文件、合同约定及国家/行业现行标准。

2.6.8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纪律要求

2.7.1评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标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评标过程和结果。对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2投标人不得具有的情形（实质性要求）

一、有下列情形之一的，视为投标人串通投标：

（一）不同投标人的投标文件由同一单位或者个人编制；

（二）不同投标人委托同一单位或者个人办理投标事宜；

（三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（五）不同投标人的投标文件相互混装。

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照采购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。

投标人有上述情形的，按照规定追究法律责任，具备一至十一条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

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投标人有下列利害关系之一的，应当回避：

（1）参加采购活动前3年内与投标人存在劳动关系；

（2）参加采购活动前3年内担任投标人的董事、监事；

（3）参加采购活动前3年内是投标人的控股股东或者实际控制人；

（4）与投标人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；

（5）与投标人有其他可能影响政府采购活动公平、公正进行的关系。

投标人认为采购人员及相关人员与其他投标人有利害关系的，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，供应商对招标文件中采购需求的询问、质疑由 秦汉项目管理有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由秦汉项目管理有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 秦汉项目管理有限公司 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、不影响投标文件的编制的情形）。

四、供应商认为采购文件、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）质疑书正本1份（政府采购供应商质疑函范本详见附件）；

（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（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：任英沛

联系电话：18700895616

地址：陕西省西安市雁塔区陕西省西安市曲江新区雁展路莱安中心T3栋403室

邮编：710000

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采购文件、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）。

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”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。）

（注：当采购包的评标方法为最低评标价法时带“★”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。）

3.1采购项目概况

按照中省国产化适配迁移任务要求，为加快提升我市政务云平台安全保障能力，有效保障政务云平台和上云政务信息系统安全稳定运行，我们将新增防火墙、威胁情报网关、综合网管系统等网络安全设备和系统，续保现有入侵防御系统、远程安全评估系统等安全设备，构建政务云平台互联网区和政务外网区双区域网络边界安全防护体系；新建1套网络安全态势感知平台，配套探针和日志审计系统，实现政务云平台双区全域安全态势可视、威胁精准识别；新建政务云平台政务外网区、互联网区云安全资源池，为全市各级各部门上云政务信息系统提供主机安全、日志审计等安全组件，实现专属安全服务。通过构建一个功能完备的纵深防护体系，将极大提升政务云平台安全防护能力和预警监测能力，有力支撑全市政务信息系统迁移上云合规要求，为全市数字政府建设与经济社会高质量发展提供坚实可靠的安全保障。

3.2采购内容

采购包1:

采购包预算金额（元）: 6,881,018.00

采购包最高限价（元）: 6,881,018.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否核心产品	是否允许进口产品	是否属于节能产品	是否属于环境标志产品	是否实施本国产品政策
1	防火墙（互联网区）	1.00	35,000.00	台	工业	否	否	否	否	是
2	数据库审计系统（互联网区）	1.00	100,000.00	台	工业	否	否	否	否	是
3	抗DDOS服务（互联网区）	1.00	210,000.00	套	软件和信息技术服务业	否	否	否	否	是
4	数据防泄漏系统（互联网区)	1.00	140,000.00	台	工业	否	否	否	否	是
5	威胁情报网关（互联网区）	1.00	200,000.00	台	工业	否	否	否	否	是
6	Web防火墙(互联网区）	1.00	114,000.00	台	工业	否	否	否	否	是
7	综合网管系统（互联网区）	1.00	180,000.00	套	软件和信息技术服务业	否	否	否	否	是
8	全流量审计（互联网区）	1.00	140,000.00	台	工业	否	否	否	否	是

9	堡垒机（互联网区）	1.00	150,000.00	台	工业	否	否	否	否	是
10	Web防火墙(政务外网区）	1.00	114,000.00	台	工业	否	否	否	否	是
11	数据库审计系统（政务外网区）	1.00	100,000.00	台	工业	否	否	否	否	是
12	数据防泄漏系统（政务外网区)	1.00	150,000.00	台	工业	否	否	否	否	是
13	综合网管系统（政务外网区）	1.00	180,000.00	套	软件和信息技术服务业	否	否	否	否	是
14	堡垒机（政务外网区）	1.00	150,000.00	台	工业	否	否	否	否	是
15	接入交换机（互联网区、政务外网区）	4.00	60,000.00	台	工业	否	否	否	否	是
16	镜像交换机（互联网区、政务外网区）	2.00	60,000.00	台	工业	否	否	否	否	是
17	网闸（互联网区、政务外网区之间）	2.00	360,000.00	台	工业	否	否	否	否	是
18	边界安全设备维保服务	1.00	540,000.00	项	软件和信息技术服务业	否	否	否	否	是
19	网络态势感知平台	1.00	500,000.00	套	软件和信息技术服务业	是	否	否	否	是
20	APT攻击监测探针（互联网区、政务外网区）	2.00	300,000.00	台	工业	否	否	否	否	是
21	日志审计（互联网区、政务外网区）	2.00	127,600.00	台	工业	否	否	否	否	是
22	云安全资源池（互联网区）	1.00	1,010,000.00	套	软件和信息技术服务业	否	否	否	否	是
23	云安全资源池（政务外网区）	1.00	1,760,000.00	套	软件和信息技术服务业	否	否	否	否	是
24	系统集成	1.00	200,418.00	项	其他未列明行业	否	否	否	否	是

3.3技术要求

采购包1:

标的名称：防火墙（互联网区）

序号	参数性质	技术参数与性能指标
1		1、标准2U机架设备，配置国产化操作系统和国产化CPU，交流冗余电源，RJ45串口≥1，RJ45管理口≥1，USB接口≥2，千兆电口≥6个（至少一组Bypass）,千兆光口≥8个（按需配置光模块），万兆光口≥4个（按需配置光模块），接口扩展槽位≥1个，内存≥32G，固态硬盘≥256G，机械硬盘≥4T，整机吞吐量≥20G，应用层吞吐量≥16G，最大并发连接数≥300万，新建连接数≥20万； ▲2、为保证产品在多项安全防护能力开启后的实际防护性能，要求产品采用多核分布式安全操作系统，充分发挥硬件的并行计算能力，需提供计算机软件著作权登记证书； ▲3、可与现网设备实现双机主备部署，并能够自动进行配置同步。 4、支持通过ICMP、TCP、UDP协议，完成对目的IP地址（支持IPv6）可达性的探测，支持在策略路由、GRE隧道、DNAT策略、HA中设置链路探测。 5、为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略。 6、黑白名单内容支持IP地址（可直接写入或通过文本智能提取）、协议TCP/UDP/ICMP和端口进行设置，且支持配置双向地址。 7、文件传输协议，支持基于HTTP、FTP、POP3、SMTP、IMAP协议的进行多线程下载以及有密码压缩包下载限制。 8、支持XFF解析功能，针对Web应用代理场景，可以解析出报文中真实客户端的IP地址。 9、支持基于域名的防火墙策略，一条策略中支持同时配置≥128个域名（支持IPV6），支持通配符格式的域名如*.test.com，支持≥10级域名且层级可配置。 10、基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑。 ▲11、为保证项目交付质量和售后服务质量，要求投标产品厂商具备履约能力相关认证和售后服务能力相关认证证书。 ▲12、为保证产品CPU、内存、硬盘等硬件的安全性和稳定性，要求产品制造商能够主动识别、分析并控制供应链中的潜在风险，如盗窃、破坏、网络攻击、供应中断等，具备供应链安全管理体系相关证书或第三方检测报告。 13、提供三年原厂质保及系统升级服务。

标的名称：数据库审计系统（互联网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，配置国产化操作系统和国产化CPU，含交流冗余电源，USB接口≥2，RJ45串口≥1，GE管理口≥1，千兆光口≥4（按需配置光模块），GE电口≥6，接口扩展槽位≥2，内存≥32G， SATA硬盘≥4TB，网络层吞吐量≥5000Mbit/秒，SQL语句处理能力≥40000条/秒，满足各类法令法规（包含等保2.0）对数据库安全的要求； 2、支持旁路阻断功能（非串联方式），两种阻断模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。 3、内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等风险审计规则库，无需单独配置，直接调用。 4、提供三年原厂质保及系统升级服务。

标的名称：抗DDOS服务（互联网区）

序号	参数性质	技术参数与性能指标

1		1、提供DDOS攻击防护≥10G清洗能力，防护IP数量≥256个； 2、基于统计攻击特征行为的识别和阻断功能,以及正常流量处理、攻击特征库维护、安全管理及日志审计等功能； 3、具备流量清洗溯源能力，支持基于SRv6的流量清洗服务，可实现靠近DDoS攻击源的DDoS攻击防护溯源； 4、具备可提供针对防护IP地址（段）的流量压制路由服务，基于端侧、城域网、骨干网多级联动流量牵引； 5、支持基于需防护目的IP地址实现分方向的流量压制功能； 6、可提供弹性防护能力，10Gbps≤弹性防护能力≤100Gbps的DDoS弹性防护能力； 7、提供三年系统服务。

标的名称：数据防泄漏系统（互联网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，千兆电口≥6个、≥4个千兆光口（按需配置光模块）；国产操作系统，CPU：国产cpu；内存：≥64G；硬盘≥4T，冗余电源，≥2个扩展槽位，7层最大吞吐≥2.5Gbps（单条策略测试性能）、7层检测吞吐≥1Gbps。 2、提供网络监控和网络阻断功能。支持常见网络协议的分析与还原，包括HTTP、FTP、SMTP/POP3/IMAP、SMB等。 3、支持针对敏感文件泄漏的链路进行流转测绘，支持记录外发敏感文件所属源区域、目的区域、文件名称、文件大小、文件类型、流转方式、文件MD5、泄漏途径、泄漏应用、文件分类、文件分级、留存位置、敏感数据量等信息，针对该泄漏文件能够在世界地图上进行流转测绘，详细标注数据路径地； 4、支持对MPLS、VLAN、VXLAN、IPv6、GRE、双栈封装、ERSPAN等协议流量进行协议识别和内容识别，并且能够在Web对上述协议的识别进行控制； 5、提供三年原厂质保及系统升级服务。

标的名称：威胁情报网关（互联网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，国产操作系统，国产CPU≥4核，≥16G内存，≥1T硬盘，管理口≥1个，配置双电源，≥4千兆电口，≥2个万兆光口（按需配置光模块）。 2、支持APT情报信息，告警信息可关联APT标签，并提供APT组织名称、攻击手法等信息。支持恶意软件、勒索、矿池、钓鱼类的域名或IP检测。支持威胁情报+入侵检测双引擎检测，吞吐量≥8Gbps。提供失陷检测情报数量不低于300万； ▲3、支持云地联合情报下发，每日通过大数据对云端亿级别情报进行定向追踪，不上传用户本地流量数据的前提下，通过用户互联网出口ip地址，及时发现用户外联境外恶意服务器的问题，并将用户特有失陷威胁情报下发至本地设备； 4、支持基于netflow、DNS等数据的威胁情报活跃度计算，给出的情报根据活跃度提取top500万； 5、情报碰撞告警提供包括告警类型、告警事件名称、告警等级、告警描述、是否APT、是否重保等告警信息； 6、提供三年质保及系统升级服务。

标的名称：Web防火墙(互联网区)

序号	参数性质	技术参数与性能指标

1		▲1、标准机架设备，国产化操作系统，国产CPU，硬盘4T机械硬盘+256G固态硬盘；配置≥2个接口扩展槽位（可用于扩展接口），配置≥8个千兆光口（按需配置光模块），≥8个千兆电口，≥4个万兆光口（按需配置光模块）。 2、吞吐量≥40G，HTTP吞吐≥15G，HTTP新建≥15W，HTTP并发连接数≥600万。 ▲3、可与现网设备实现双机主备部署，并能够自动进行配置同步。 4、支持SSL透明代理，可以对HTTPS 国密网站进行保护，一个站点同时防护国密及商密网站,需提供具备CMA或CNAS资质的第三方测评机构出具的检测报告。 5、系统具备跨站攻击防御能力，可以对XSS和CSRF攻击进行防御。 6、系统具备Web访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，支持基于扫描防护。 7、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略。 8、提供丰富的日志信息。 9、提供集中展示功能。 ▲10、支持页面动态混淆防护，在保证业务和页面展示效果的情况下，对响应页面中的Form表单、a标签、Javascript文件等关键信息进行混淆，支持对例外URL不进行混淆操作，需提供具备CMA或CNAS资质的第三方测评机构出具的检测报告。 ▲11、为保证产品CPU、内存、硬盘等硬件的安全性和稳定性，要求产品制造商能够主动识别、分析并控制供应链中的潜在风险，如盗窃、破坏、网络攻击、供应中断等，具备供应链安全管理体系相关证书或第三方检测报告。 12、提供3年原厂维保及WAF特征库升级服务。

标的名称：综合网管系统（互联网区）

序号	**参数性质**	**技术参数与性能指标**

1		▲1、通过资源树统一管理网络内所有设备，系统支持对网络设备，服务器，安全设备，数据库，中间件，应用服务，链路等资源监控，真实实反映设备，资源运行的健康度和运行情况,授权数量≥300个。 2、统一管理网络内所有设备，真实反映设备资源的状态和性能运行情况，构建资源多维度的指标监控，及时了解设备运行情况。 3、通过告警级别，事件/故障类型，设备类型，指定时间段等关键字进行查询和统计查看设备实时和历史运行情况。 4、系统能支持跨厂商跨平台监控，支持多厂商设备组成的混合网络自动发现。包含基本的首页概况，资源监控管理，拓扑管理，告警管理，报表分析，网络工具，发现管理，策略管理，通知管理等产品配套基础功能，实现对所有IT资源和网络设备的全面监控。 5、集成全网运行情况、故障等信息统一展示；图形化展示各类资源统计信息；支持将监控的设备指标、拓扑图等自定义展示到大屏；支持界面轮播，灵活部署多屏展示；支持不同分辨率，可调整界面文字大小，自定义配置多界面轮播的轮播间隔时间。 6、拓扑支持分层分级展现，可设置父子级收缩关系，快速展开下级拓扑；同一拓扑图支持建立分区、分组，可收缩展开，收缩时显示下级异常，通过指示灯和数字提醒，提供分组名称自定义。机柜拓扑图展示：支持自定义多个机柜拓扑图，可视化拖动部署，可添加真实和非网管示意设备，展示设备状态与运行情况，可打开设备背板定位异常，展示机柜配置和布局数据。 7、支持设备与设备之间的依赖关系，上下游关联性依赖关系，依附从属性依赖关系-自动生成服务器与应用的关系，方便直观展现所有承载数据库、中间件、服务应用的主机关系和实时状态监控。 8、内建多种数据展示模板智能匹配，提供多种类型组件，界面数据自定义选择配置，搭配图形化编辑界面，拖拽功能，满足多种展示场景。支持告警数据下钻。当大屏幕上的故障组件出现异常提醒，可通过可视化平台进行页面下钻，快速跳转到异常列表。 9、系统首页框架可自定义，基于全局视角设计运维看板，系统支持为不同权限人员设置重点关注组件，支持多种页面布局切换，支持组件拖拽调整位置，单个页面可配置多个组件。 10、提供三年维保及系统升级服务。

标的名称：全流量审计（互联网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，国产化操作系统，国产化CPU;内存≥64G,吞吐量≥1Gbps,数据检索速度≥50TB/秒； 接口配置≥5个千兆电口，≥4个千兆光口（按需配置光模块），冗余电源，≥24TB容量硬盘。 2、支持手动和FTP方式批量导入PCAP包对离线流量采集，文件大小不低于1个G；并记录PCAP包导入记录及检测状态。 3、支持灵活开启机器学习模型，增强检测精度，模型至少包括：ICMP隧道检测、DNSTunnel检测、HTTP隧道检测、CS流量检测、MSF检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH爆破登录成功检测。 4、提供三年硬件维保和技术支持服务。

标的名称：堡垒机（互联网区）

序号	参数性质	技术参数与性能指标

1		▲1、标准机架式设备，配置国产化操作系统和国产化CPU，含交流冗余电源，≥128G固态系统盘，≥16T机械数据盘，≥6*千兆电口，≥4*千兆光口（按需配置光模块），≥2*USB，≥1*串口，≥1*GE管理口，≥1*GE热备口，≥2*扩展插槽，硬件国密加密卡，配置≥300个资产授权，≥3个SDP远程并发接入授权，字符最大并发会话数≥4500，图形最大并发会话数≥2500； 2、系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置，防止密码泄露不支持找回； 3、用户登录堡垒机支持多种认证方式，包括本地静态密码认证、短信认证等身份认证方式；支持可知因素和不可知因素的双因素认证； ▲4、支持通过堡垒机直接代理HTTP/HTTPS协议，无需前置机；提供具备CMA或CNAS资质的第三方测评机构出具的检测报告； ▲5、支持达梦、人大金仓等数据库协议代理，支持调用本地工具运维，保留运维习惯。提供具备CMA或CNAS资质的第三方测评机构出具的检测报告； 6、支持基于用户、用户组、组织机构、角色和用户属性的静态授权，通过不同授权模型满足运维管控要求； 7、支持RDP、SSH、TELNET、SFTP、FTP等协议的HTML5运维，无需本地运维客户端； 8、支持自动化运维功能，支持linux shell脚本、python脚本等脚本类型； ▲9、为保证产品CPU、内存、硬盘等硬件的安全性和稳定性，要求产品制造商具备供应链安全管理体系相关认证证书或第三方检测报告； 10、提供三年原厂质保及系统升级服务。

标的名称：Web防火墙(政务外网区)

序号	参数性质	技术参数与性能指标
1		▲1、国产化操作系统，国产CPU，硬盘4T机械硬盘+256G固态硬盘；配置8个千兆光口（按需配置光模块），8个千兆电口，4个万兆光口（按需配置光模块），2个接口扩展槽位（可用于扩展接口）；吞吐量40G，HTTP吞吐15G，HTTP新建15W，HTTP并发连接数600万； 2、支持SSL透明代理，可以对HTTPS 国密网站进行保护，一个站点同时防护国密及商密网站； 3、系统具备注入攻击防御能力，可以对SQL注入、LDAP注入、SSI指令注入、Xpath注入、命令注入、远程文件包含以及其他注入进行防御； 4、系统具备跨站攻击防御能力，可以对XSS和CSRF攻击进行防御； 5、系统具备Web访问控制能力，可以对扫描器的扫描行为、爬虫行为、目录遍历行为进行防御，支持基于扫描防护； 6、支持对保护站点的流量进行智能学习，并根据学习结果生成针对性的防护策略； 7、提供丰富的日志信息，包括设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、、Web访问日志等； 8、提供集中展示功能，可展示威胁事件风险分布、威胁事件类型分布、实时威胁事件、等内容； 9、支持页面动态混淆防护，在保证业务和页面展示效果的情况下，对响应页面中的Form表单、a标签、Javascript文件等关键信息进行混淆，支持对例外URL不进行混淆操作； 10、产品具备信息技术产品安全测试证书； 11、投标产品产品能够全面支持IPV4和IPV6的网络配置和安全防护； 12、产品具备《网络关键设备和网络安全专用产品安全认证证书》或《网络安全专用产品安全检测证书》； 13、投标产品符合国产化要求，提供国产化CPU和国产化操作系统的兼容性证明； 14、设备支持标准的双机主备协议，支持主备部署； 15、提供三年原厂维保及WAF特征库升级服务。

标的名称：数据库审计系统（政务外网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，配置国产化操作系统和国产化CPU，含交流冗余电源，USB接口≥2,RJ45串口≥1,GE管理口≥1，千兆光口≥4(按需配置光模块)，GE电口≥6，接口扩展槽位≥2，内存≥32G，SATA硬盘≥4TB； 2、网络层吞吐量≥5000Mbit/秒，SQL语句处理能力≥40000条/秒； ▲3、系统需支持国产数据库的审计，包括达梦、人大金仓等国产数据库及其主流版本（需提供功能截图或其他证明材料）； 4、满足各类法令法规(包含等保2.0等)对数据库安全的要求； 5、系统需支持多维度组合审计查询，查询条件包括时间、报文、资产等； 6、系统需支持SQL性能趋势分析，可统计性能变化趋势，并自动识别耗时最长、性能最差及执行量最大的SQL模板； 7、系统需支持旁路镜像流量方式部署，无需在被审计数据库主机上安装任何代理程序即可完成审计；同时需支持在数据库主机侧部署采集组件，以满足云环境、虚拟化环境等内部流量无法镜像场景下的审计需求； 8、系统需支持对CPU、内存、硬盘使用率的告警阈值进行设置；分布式部署时支持对各采集节点分别设置不同的阈值； 9、系统需支持记录自身报表外送、通知发送等自动触发行为的操作日志，满足审计追溯要求； 10、提供三年原厂质保和软件升级服务。

标的名称：数据防泄漏系统（政务外网区)

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，千兆电口≥6个、≥4个千兆光口(按需配置光模块);国产化操作系统、CPU：国产化cpu；内存:≥64G、硬盘≥4T，冗余电源，≥2个扩展槽位； 2、7层最大吞吐≥2.5Gbps(单条策略测试性能)、7层检测吞吐≥1Gbps； 3、系统需支持常见文件类型与内容的识别，包括办公类（doc、docx、xls等）、图片类（jpg、jpeg、png等）、压缩类（rar、zip等），支持自定义压缩包递归解析层数； 4、系统需内置常见敏感数据正则识别规则，包括身份证、银行卡、手机号、车牌号、护照等； 5、系统需配置压缩包解析层数、文件解析超时时长、文件最大识别容量、内容快照字数上限、数据传输方向、单张图片检测范围等参数； 6、系统需支持 IPv4、IPv6 双栈环境，可解析 HTTP、HTTPS、SMTP、SMTPS、POP3、POP3S、IMAP、FTP、SMB、NFS、TELNET、DNS即时通讯离线文件传输等协议，并对协议承载业务数据进行内容还原；协议识别基于协议特征实现，不依赖固定端口； 7、支持自定义关键词或关键词组检测策略，可选择存在性检测、匹配次数统计、匹配类别数量统计多种检测模式；支持配置邻近关联关键词检测规则； 8、系统需自定义报表，可按需选择分析维度生成报表并支持预览； 9、系统需支持审计日志展示与检索，采用列表形式，以格式化字段展示流量还原后的审计日志； 10、提供网络监控或网络阻断功能； 11、提供三年原厂质保和软件升级服务。

标的名称：综合网管系统（政务外网区）

序号	参数性质	技术参数与性能指标

1		▲1、通过资源树统一管理网络内所有设备，系统支持对网络设备，服务器，安全设备，数据库，中间件，应用服务，链路等资源监控，真实实反映设备，资源运行的健康度和运行情况,授权数量≥300个。 2、统一管理网络内所有设备，真实反映设备资源的状态和性能运行情况，构建资源多维度的指标监控，及时了解设备运行情况。 3、通过告警级别，事件/故障类型，设备类型，指定时间段等关键字进行查询和统计查看设备实时和历史运行情况。 4、系统能支持跨厂商跨平台监控，支持多厂商设备组成的混合网络自动发现。包含基本的首页概况，资源监控管理，拓扑管理，告警管理，报表分析，网络工具，发现管理，策略管理，通知管理等产品配套基础功能，实现对所有IT资源和网络设备的全面监控。 5、集成全网运行情况、故障等信息统一展示；图形化展示各类资源统计信息；支持将监控的设备指标、拓扑图等自定义展示到大屏；支持界面轮播，灵活部署多屏展示；支持不同分辨率，可调整界面文字大小，自定义配置多界面轮播的轮播间隔时间。 6、支持监控展示页对监控对象展示总览、系统展示和预留扩展页；应支持Tab重命名、拖动排序、布局持久化，以及蜂巢/色块两种状态视图。 7、支持创建自定义视图、设计多层节点树、为节点配置模型与过滤条件，并按角色控制节点可见性，形成结构化的CI展示入口。 8、建立各类信息化资源的运维档案，能够记录各个软件及硬件资源的运维历史，包括排障记录、变更记录、服务记录等。 9、支持主流国产化服务器的硬件监测，支持对各个主流品牌服务器硬件的风扇、电源、硬盘及温度的状态监测，同时支持SNMPV1/V2/V3、WMI、SSH、TELNET协议。 10、提供三年维保及系统升级服务。

标的名称：堡垒机（政务外网区）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，配置国产化操作系统和国产化CPU，含交流冗余电源，≥32G内存，≥4T数据盘，≥4*千兆电口，≥4*千兆光口（按需配置光模块），≥2*USB，≥1*串口，≥1*GE管理口，≥1*扩展插槽，硬件国密加密卡； 2、配置≥300个资产授权，字符最大并发会话数≥2000，图形最大并发会话数≥500； 3、需支持主流运维协议接入，兼容SSH、TELNET、RDP、FTP、SFTP等常用运维传输协议，满足各类设备远程运维接入需求； 4、需支持用户会话并发数量管控，可自定义单用户最大并发运维会话数量，有效规避超额占用运维资源的问题，保障平台运维资源合理分配； 5、需支持全方位运维审计管控能力，可对运维操作录像、键盘输入行为、文件传输操作、字符交互日志、数据库双向访问行为等各类运维行为进行全程记录与合规审计管控； 6、需支持浏览器运维模式，可开展SSH、TELNET、FTP、SFTP等协议运维操作，无需安装本地客户端工具，实现轻量化、无插件远程运维； 7、需支持Web应用账号自动化改密能力，搭载可视化改密配置向导，可通过配套扩展工具自动生成适配各类Web业务系统的改密执行脚本，实现Web业务账号密码自动化轮换更新； 8、需支持多维度运维数据分析报表统计，可基于运维次数、运维时长、在线活跃时长、会话规模、命令交互数量、文件传输数量、来源访问地址、运维时间分布等维度自动生成统计报表；报表支持PDF、DOC、HTML等通用格式导出，满足合规汇报与态势分析需求； 9、需支持平台告警日志及运行状态信息外送，可通过邮件、Syslog、企业协作平台等方式推送告警信息，支持自定义日志告警级别；支持通过SNMP协议输出平台运行状态数据，适配各类运维监控平台对接； 10、提供三年原厂质保和软件升级服务。

标的名称：接入交换机（互联网区、政务外网区）

序号	参数性质	技术参数与性能指标
1		1、接入交换机，支持堆叠，支持IPv6；≥48个10GE 光口（按需配置光模块），≥6个40GE 光口（按需配置光模块），AC冗余电源；交换容量≥2.16Tbps，包转发率≥1071Mpps； 2、提供三年原厂质保及硬件维保服务。

标的名称：镜像交换机（互联网区、政务外网区）

序号	参数性质	技术参数与性能指标
1		1、镜像交换机，≥4个万兆SFP+光口（按需配置光模块），≥24个千兆SFP光口（按需配置光模块），整机吞吐性能≥128Gbps，支持接收交换机镜像或分光采集后流量进行复制/汇聚/Hash分流，双冗余电源AC220V； 2、提供三年原厂质保及硬件维保服务。

标的名称：网闸（互联网区、政务外网区之间）

序号	参数性质	技术参数与性能指标
1		▲1、2U型机架设备，配置国产化操作系统和国产化CPU，含交流冗余电源，内外网端机分别≥1*4T硬盘、≥2*电口(M或HA)、≥4个千兆电口，≥4个万兆SFP插槽(按需配置光模块)和≥4个千兆SFP插槽(按需配置光模块)、≥2个扩展插槽（用于扩展接口）、≥2*USB接口、≥1*串口； ★2、最大并发连接数≥100万，吞吐量≥10Gbps； 3、支持跨域访问(邮件、网页、文件、数据库、远程访问)、数据库同步、文件同步、关键字过滤等功能； 4、系统需支持多类主流文件传输及同步协议，包含远程FTP、FTPS、SFTP及本地FTP、SFTP、TFTP协议，同时支持客户端接入模式，可实现跨安全区域的文件交换与数据同步业务； 5、系统需支持不同安全等级网络区域间的数据交互能力，可实现高安全区域与低安全区域之间的单向、双向文件同步与数据交换，满足跨域合规数据流转业务需求； 6、系统需支持数据同步自定义条件过滤，可根据业务需求自定义数据筛选规则，仅允许符合条件的数据参与传输同步，支持标准条件语句自定义过滤逻辑，精准管控同步数据范围； 7、系统需支持精细化访问控制策略配置，可自定义允许或拒绝外部主体访问内部业务服务，支持基于访问协议、传输方向、源IP、源端口、目的IP、目的端口、匹配关键字等多维度组合配置访问管控规则； 8、系统需具备基础网络攻击防护能力，可针对CC攻击、缓冲区溢出攻击、ICMP超大包攻击、TCP、UDP、ICMP泛洪攻击进行阈值检测与流量管控，有效抵御常见网络异常攻击行为； 9、系统需支持基于时间策略的访问控制能力，可配置每日、每周、每月固定周期策略，亦可自定义专属时间区间，实现分时段精细化安全访问管控； 10、支持双机主备部署； 11、提供三年原厂质保和软件升级服务。

标的名称：边界安全设备维保服务

序号	参数性质	技术参数与性能指标

序号	设备名称	技术参数	单位	数量

1			1	防火墙（政务外网区）	设备型号：NFNX3-ZA 提供自合同签署后≥3年软件系统及特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	2
			2	入侵防御系统(政务外网区)	设备型号：NIPSNX5-HFA（万兆） 提供自合同签署后≥3年软件系统及入侵防御特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	2
			3	入侵检测系统（政务外网区）	设备型号：NIDSNX5-HFA（万兆） 提供自合同签署后≥3年软件系统及入侵检测特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	1
			4	远程安全评估系统（政务外网区）	设备型号：RSASNX3-HFB 提供自合同签署后≥3年软件系统及漏洞库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	1
			5	入侵防御系统（互联网区）	设备型号：NIPSNX3-ZA 提供自合同签署后≥3年软件系统及入侵防御特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	1

6	web应用防火墙（互联网区）	设备型号：WAFNX5-HF 提供自合同签署后≥3年软件系统及web防护特征库升级服务。服务期内，提供最新产品补丁和产品规则文件升级服务，用户可随时获得软件的最新补丁及规则库的升级文件；对软件缺陷，需采用补丁软件进行维修、提供升级软件予以更换或以退款方式进行处理；当产品许可证文件丢失时，能够重新提供新的许可证，以保证客户的产品能够正常使用。 提供自合同签署后≥3年产品硬件保修服务。服务期内，提供产品的免费维修和超时提供替换用机的服务。产品在出现故障并且经过产品生产厂商技术支持中心确认为产品故障时，客户可将产品送至产品生产厂商技术支持中心，在收到客户提供的故障产品后 15 个工作日（不含运输时间）内修复并快运给客户；如15个工作日内无法修复该故障产品，将为客户免费提供与返修产品功能一致的产品暂时替换，直至故障产品修复。 服务期内，提供远程支持服务，包括远程受理和解决产品问题、资料提供和其他应用咨询等内容。	台	1
7		▲按以上 6 类设备维保服务要求，提供完整维保服务承诺函，承诺函须加盖供应商或厂商公章；		

标的名称：网络态势感知平台

序号	参数性质	技术参数与性能指标
		1、汇总展示网络安全态势相关关键指标； 2、支持资产管理，平台内置常见基础资产类型，支持实现资产全生命周期管理； 3、支持资产新增、删除、编辑等操作；支持导入方式新增资产； 4、支持以不同组织架构视角查看资产数据；支持管理员查看所有组织架构的资产数据；支持子账号仅显示其权限范围内的资产； 5、支持自定义配置资产字段信息； 6、支持对资产、漏洞、业务的逻辑整合展示，可基于多个视角，查看核心业务的风险情况； 7、支持漏洞管理能力，可对接常见漏洞扫描设备，支持多维展示漏洞数据，支持漏洞全生命周期运营，支持从漏洞风险识别到闭环的全流程管理能力； 8、支持与态势感知探针等联动，同步资产至平台资产管理模块； 9、支持资产与组织关联，支持资产与告警、原始日志等数据关联；支持资产与漏洞关联； 10、支持安全事件的全生命周期管理，支持事件关联分析能力，还原攻击过程的关键节点与时间线； 11、支持对接现网安全设备日志，实现对多维度数据的全面汇聚，采用多种技术手段策略，快速精准识别各类潜在威胁，支持展示告警详情； 12、支持查看告警的基本信息、处置响应、举证全文信息，支持查看对应视图； 13、支持多种内置安全分析场景； 14、支持添加白名单，支持自定义白名单条件及生效时间； 15、支持多种语法查询日志，支持嵌套查询，支持检索条件保存、检索历史记录记录查看； 16、支持日志可视化分析查询，可实现自定义分析统计； 17、支持自动化处置响应能力，可留存响应历史记录，支持自动或手动阻断指定IP对目标系统与网络的访问； 18、支持重大活动保障，支持重大活动全阶段细化管理； 19、支持平台本地情报查询，可查询展示情报详情信息； 20、支持威胁情报源管理与更新，支持对接第三方威胁情报源，支持情报在线或离线更新； 21、支持全生命周期管理安全工单管理，用户可发起工单、跟踪工单流转状态，实现安全事件处理流程的规范化、可视化管理； 22、支持展示与管理对应操作权限的平台工单，支持对工单的细化管控； 23、支持安全分析模型配置和管理能力，内置多种告警分析模型，支持自定义新增模型，支持自定义分析模型； 24、支持基于多源条件，灵活设定触发规则，设定事件触发或周期触发；当系统达到预设

1		条件后，将自动关联运行处置剧本，提升处置响应效率； 25、支持可视化的自动化处置响应编排，并实现全生命周期管理；支持满足复杂业务场景下的流程编排需求； 26、支持与现网防火墙等常见安全设备联动，或人工选择联动实现攻击地址自动封禁； 27、支持多种日志接入方式，支持日志源重识别、数据过滤、去重等； 28、根据业务需求按部门、业务等多层级划分组织架构，支持组织用户信息管理； 29、支持根据业务需求划分安全域，将资产等按实际需要纳入不同的安全域； 30、支持升级管理，支持升级记录； 31、支持安全态势可视化呈现，以大屏的方式从多维度进行可视化展示； 32、支持根据对可视化大屏基于当前登录用户权限展示对应数据范围，支持自定义大屏轮播时间和顺序； 33、支持以地图动态可视化展示攻击来源地域分布、告警量；支持按照攻击各阶段展示多维告警详情；支持展示攻击、受攻击情况； 34、支持可视化展示横向的异常访问数量、正常访问数量、累计流量统计；支持展示内外部受攻击排行、攻击方向、攻击排行等； 35、支持可视化展示外连威胁风险；支持按照时间和组织维度进行筛选展示； 36、支持可视化展示现网资产同比变化情况，并以多维形式展示风险资产占比、告警、风险趋势等； 37、支持可视化展示Web访问数据统计，可展示攻击、被攻击地址、类型、趋势； 38、支持可视化展示当前资产、告警、漏洞情况，并支持展示对应详情数据、实时攻击统计等； 39、支持可视化展示多种维度的网络实体关系态势，可分析展示实体访问方向、下钻查看详情； 40、支持可视化展示资产安全情况，包括常见多维数据； 41、支持可视化展示攻击者基本信息、攻击详情等； 42、支持通过邮件、短信等多种方式进行消息通知； 43、内置多种报告模板，支持手动生成和自动订阅，可设定报告发送周期和生成时间； 44、支持平台资源利用率监控；支持对各组件运行健康状态的集中监控； 45、支持对接入的安全探针进行统一管理，支持查看探针状态，支持一键升级； 46、支持平台开放API接口管理，第三方可通过API获取平台的接口信息进行对接； 47、支持用户角色管理，支持配置各角色对应的菜单权限； 48、平台定制费用，含可视化展示、与云安全资源池对接、与现网设备对接、接口开发定制、根据现状适配优化功能等； 49、支持常见协议类型的日志采集能力，支持日志数据过滤、标准化解析，支持日志解析规则匹配及性能监控； 50、提供综合威胁分析、主机威胁分析、外部威胁分析等多个智能报表；提供综合管理和关联分析能力； 51、支持与APT攻击监测探针、日志审计等设备联动，实现统一流量分析和安全预警； 52、提供三年原厂维保服务。

标的名称：APT攻击监测探针（互联网区、政务外网区）

序号	参数性质	技术参数与性能指标

1		▲1、软硬一体≥2U机架式设备，CPU：国产化，CPU数量≥1；操作系统：国产化操作系统；Console口≥1个；USB：USB2.0≥2；内存：≥32G；硬盘：≥2T；网络接口：管理口≥1千兆电，业务口≥4千兆电，≥2万兆光（含2个万兆多模光模块）；电源规格：1+1冗余电源； 2、整机吞吐量≥5Gbps； 3、通过流量采集技术捕获网络通信数据，结合智能分析引擎与威胁情报库，对漏洞利用、木马、黑客攻击等未知威胁进行深度检测（需提供功能截图或其他证明材料）； 4、支持对各种WEB攻击、邮件社工类攻击进行检测； 5、支持多维度全方位发现失陷主机；识别内网中横向扩散及渗透攻击行为； 6、支持对检测对象的会话特征进行多维度监控统计； 7、支持对流量中的资产进行统计分析； 8、支持自定义抓包分析能力，可基于IP、端口、协议类型等条件配置抓包任务，抓取的原始流量数据包可本地留存，用于事后分析、事件取证与溯源核查； 9、支持双向流量审计，需提供对请求和响应内容进行审计； 10、支持与网络安全态势感知平台联动，能够将探针收集的数据上传到态势感知平台； 11、提供三年原厂质保和软件升级服务。

标的名称：日志审计（互联网区、政务外网区）

序号	参数性质	技术参数与性能指标
1		▲1、软硬一体≥2U机架式设备；CPU：国产化CPU，CPU数量≥1；操作系统：国产化操作系统；Console口：1个；USB：USB2.0≥2；内存：16G内存≥1；硬盘：4T硬盘≥1；电源规格：1+1冗余电源；网络接口：业务口（千兆电）≥4个，业务口（千兆光）≥4个（按需配置光模块），管理口(千兆电)≥1个；接口扩展槽≥2个； 2、授权资产数≥500个；数据平均处理能力≥10000EPS； ▲3、针对分散的异构日志进行集中采集、统一管理、存储与统计分析，可协助满足等保合规要求。其核心功能包括：支持多源日志接入，覆盖网络设备、安全设备、操作系统、数据库、应用系统等，通过Syslog、SNMP、Agent等多种协议或工具实现全面采集（需提供功能截图或其他证明材料）； 4、提供日志标准化处理，对不同格式的原始日志进行清洗、解析和字段归一化，确保后续分析的一致性； 5、具备实时日志分析能力，通过预设规则对接入的日志进行实时分析； 6、支持日志存储合规；提供高效检索功能，支持按时间范围、设备类型、事件类型、关键词等多维度检索，支持模糊查询和复杂条件组合查询； 7、内置关联分析模型，通过关联规则挖掘潜在的安全事件； 8、支持生成丰富的合规报表，支持自定义报表模式，满足实时报表、周期性任务报表等需求； 9、具备日志转发能力，可通过本系统日志转发机制，将采集日志同步转发至其他日志存储及分析设备； 10、支持与网络安全态势感知平台联动，能够将日志审计收集的日志上传到态势感知平台； 11、提供三年原厂质保和软件升级服务。

标的名称：云安全资源池（互联网区）

序号	参数性质	技术参数与性能指标
		序号 / 设备名称 / 技术参数 / 单位 / 数量

		1	基础功能	1、支持对资源池状态进行总览 2、支持列出全部物理资源和虚拟资源信息，除基本信息外，还展示单机实时服务状态、实时告警数量、实时CPU、内存、磁盘使用率 3、支持创建、删除、编辑云租户单位 4、支持对云租户单位内部用户新增、删除等管理 5、支持为云租户单位直接开通云安全组件，或设置云安全组件配额 6、支持云租户用户创建、导入、删除、重置密码等 7、支持设置云租户登录的IP、MAC黑白名单 8、支持设置云租户登录的时间访问控制 9、支持针对云租户的登录门户、认证方式、租户自管理权限等设置 10、支持查看和管理所有云安全组件产品开通情况、状态 11、支持直接单点登录至对应云安全组件进行管理 12、支持部署云安全组件对应的系统实例 13、支持对云安全组件对应的实例资源规格进行变更、管理 14、支持设置云安全组件规格、自定义套餐 15、支持设置云安全组件默认开通时长、多个组件组合管理等 16、支持设置云安全组件镜像 17、IP资源池：设置云安全资源池可使用的IP段及VLANID 18、组网配置：实现云安全资源池内置防火墙等组件固定组网配置 19、网络编排配置：实现云安全资源池内置防火墙等组件网络编排接入 20、针对受保护的资产和云安全组件进行自定义流量编排 21、IPv4/IPv6双栈：支持IPv4和IPv6双栈协议 22、系统维护：支持系统自动诊断检测，支持检测各项服务的状态 23、云安全组件订单管理：支持查看和管理所有云安全组件产品开通订单情况、状态，查看开通时间、账户、订单详情等 24、工单管理：查询和管理所有云租户工单 25、工单审批：审批所有云租户工单 26、访问管理：设置云安全资源池访问方式 27、认证策略：设置认证方式、双因子认证、用户密码强度等 28、登录安全策略：支持设置访问IP、超时锁定等策略 29、日志管理：支持设置日志记录策略、日志备份策略 30、短信联动：支持设置与常见短信网关联动 31、邮件联动：支持设置邮件服务器联动 32、升级管理：平台软件升级、升级历史查询 33、规则库升级管理：云安全组件规则库导入、一键升级、升级历史查询 34、用户管理：设置云安全资源池全局的超级管理员、安全管理员、审计管理员等；支持对用户进行创建、查询、删除、重置密码 35、角色管理：支持对所有用户角色进行自定义功能授权和角色分配 36、支持查看用户登录日志、系统日志等系统级日志 ▲37、支持安全组件分配功能，管理员可直接为各个云租户分配安全资源，同时完成关键安全资源的策略初始化。（提供产品功能截图并加盖厂商公章） ▲38、支持在系统界面上动态分配安全组件性能规格，允许对已分配组件规格进行动态变更和授权回收；回收的授权可分配至其他用户或其他类型安全组件。（提供产品功能截图并加盖厂商公章） ▲39、支持配置租户安全服务链：可灵活选择流量的源、目的以及途经的安全服务节点，并可调整节点的编排顺序。（提供产品功能截图并加盖厂商公章） ▲40、安全组件可独立于平台软件进行升级，快速获取最新功能；同时支持多租户组件批量升级，显著提升运维效率。（提供产品功能截图并加盖厂商公章）	项	1

1			2	云租户管理	1、威胁概览：支持展示近期发生的安全威胁的类型，每种安全威胁的时间变化趋势，可以查看最新安全威胁事件； 2、安全概览：支持查看当前已经开通的安全组件和攻击事件数量 3、威胁分析：风险总数、当日新增风险、高危风险、web安全事件、涉及资产数的统计展示 4、自定义报表：支持自定义报表 5、报表查询：支持按报表类型、日志、名称维度对报表进行查询 6、报表下载：支持报表下载 7、日志查询：支持查询和下载租户云安全产品日志 8、云安全组件申请：支持以工单形式申请云安全组件 9、云安全组件查询：支持查询已开通的云安全组件情况和状态 10、云安全组件退订：支持对已开通的云安全组件进行退订 11、云安全组件操作：支持对已开通的云安全组件进行部署操作，可单点登录到对应云安全组件；支持重启、停止、删除云安全组件实例 12、工单管理：支持对云租户单位内部工单管理、审批 13、信息管理：支持查看和管理云租户自身单位的云安全组件开通和使用情况 14、成员管理：支持创建和管理云租户自身单位账户 15、权限管理：支持对云租户自身单位账户权限的分配、管理、授权；支持对从功能模块、账户、资产、云安全组件等维护进行权限管理 16、订单管理：支持对云租户自身所有云安全组件订单进行管理、查询 17、日志管理：支持对云租户自身的所有操作日志、使用日志等管理和查询	项	1

3	云安全组件服务-漏洞扫描	1、管理可扫描的主机、数据库、Web站点等资产 2、对主机资产进行扫描，并进行漏洞管理 3、对Web站点资产进行扫描，并进行漏洞管理 4、对数据库资产进行扫描，并进行漏洞管理 5、对主机、数据库、中间件等进行核查，提供安全整改建议 6、对主机、数据库、Web应用等进行弱口令扫描，支持自定义用户名密码字典 7、对扫描的漏洞结果进行汇总统计、展示和导出 8、提供操作日志查询、统计、分析等	采用虚拟化技术，集成网络安全、数据安全等安全能力，为用户提供一站式云安全综合解决方案。以安全资源池的方式融合多种安全能力向用户进行一站式提供，支撑云内租户单位的独立安全管理，满足各上云单位的等级保护2.0安全需求，并支持通过管理平台进行统一调度、配置、监控和分析。支持租户管理；互联网云安全资源池可支持15个上云业务单位通过等级保护2.0测评。	15
4	云安全组件服务-API审计	1、支持API接口流量审计和过滤 2、支持采集接口流量数据，支持状态监控和管理 3、支持对应用、API接口识别，可识别和划分接口类型及标签 4、支持对API接口账户的识别、提取 5、支持对API传输文件的审计、识别 6、支持API传输的常见敏感数据识别 7、支持API接口行为风险识别和预警 8、支持接口访问记录，并展示详情		
5	云安全组件服务-数据库审计	1、支持对可审计的数据库进行管理，支持国产数据库、关系型、大数据等常见数据库 2、支持审计数据库的操作类型、数据库账号、客户端IP、服务器IP、语句执行时间、返回结果等 3、支持对关于数据库的安全风险监测审计、预警，可对数据库风险操作行为、攻击行为进行告警 4、支持设置安全审计和风险监测策略，支持自定义策略 5、支持对审计数据进行多维报表统计和呈现		
6	云安全组件服务-日志审计	1、支持通过Syslog、SNMP、FTP等常见方式收集云主机资产日志 2、支持提供所采集日志数据的合规存储、查询回溯 3、支持对采集日志数据的综合统计、多维分析和呈现、导出 4、支持日志集中存储、备份、加密等策略管理 5、支持对提供日志数据的资产进行管理，支持对日志采集Agent进行管理，包括启动、停止、卸载、状态监控等		
7	云安全组件服务-主机安全	1、收集云主机所有资产信息和运行状况，包括进程、启动项、账户等详细信息 2、支持云主机防病毒，支持实时防护和主动扫描 3、支持对针对云主机的攻击行为进行防护 4、支持对黑客攻击行为进行检测，支持主机基线核查、主机风险自评估、主机账户异常行为等检测和预警，支持威胁情报匹配 5、支持主机安全日志的查询、统计、分析		
8	云安全组件服务-流量监测审计	1、支持配置安全监测策略，支持自定义策略 2、支持对流量采集进行管理，包括启动、停止、卸载、状态监控等 3、支持对常见攻击行为、恶意文件攻击行为进行检测 4、支持对攻击行为的多维查询、统计、回溯、分析		
9	云安全组件服务-Web防火墙	1、支持对保护的站点进行管理，可配置HTTP、HTTPS防护 2、支持对保护站点的跨站脚本(XSS)、注入式攻击、Webshell攻击、漏洞攻击、未授权访问等Web攻击行为防护 3、支持对常见敏感信息泄露行为进行防护，防止通过web获取服务器或后端敏感信息 4.支持基于规则的攻击防护策略，支持自定义策略 5、支持对防护日志的查询、统计、分析 6、支持记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容、cookie等内容		
10	云安全组件服务-防篡改	1、支持对各类网页的防篡改保护，包括静态和动态网页以及各类文件信息。 2、支持对指定网站目录文件夹以及子文件夹的保护，避免网站被插入恶意代码或被篡改。 3、支持对白名单规则，可支持基于目录、进程、IP、用户、时间等进行白名单访问。 4、支持网站同步发布能力，可实现网站同步发布、被篡改自动恢复。		

		11	云安全资源池定制	定制费用，含可视化展示、与态势感知平台对接、与云平台对接、接口开发定制、根据现状适配优化功能等。	项	1
		12	维保	提供三年云安全资源池原厂维保服务。	项	1
		13	交换机	接入交换机，支持堆叠，支持IPv6；≥48个10GE 光口（按需配置光模块），≥6个40GE 光口（按需配置光模块），AC冗余电源；交换容量≥2.16Tbps，包转发率≥1071Mpps；提供三年原厂质保及硬件维保服务。	台	2

标的名称：云安全资源池（政务外网区）

序号	参数性质	技术参数与性能指标

序号	设备名称	技术参数	单位	数量

		1	基础功能	1、支持对资源池状态进行总览 2、支持列出全部物理资源和虚拟资源信息，除基本信息外，还展示单机实时服务状态、实时告警数量、实时CPU、内存、磁盘使用率 3、支持创建、删除、编辑云租户单位 4、支持对云租户单位内部用户新增、删除等管理 5、支持为云租户单位直接开通云安全组件，或设置云安全组件配额 6、支持云租户用户创建、导入、删除、锁定、重置密码等 7、支持设置云租户登录的IP、MAC黑白名单 8、支持设置云租户登录的时间访问控制 9、支持针对云租户的登录门户、认证方式、租户自管理权限等设置 10、支持查看和管理所有云安全组件产品开通情况、状态 11、支持直接单点登录至对应云安全组件进行管理 12、支持部署云安全组件对应的系统实例 13、支持对云安全组件对应的实例资源规格进行变更、管理 14、支持设置云安全组件规格、自定义套餐 15、支持设置云安全组件默认开通时长、多个组件组合管理等 16、支持设置云安全组件镜像 17、IP资源池：设置云安全资源池可使用的IP段及VLANID 18、组网配置：实现云安全资源池内置防火墙等组件固定组网配置 19、网络编排配置：实现云安全资源池内置防火墙等组件网络编排接入 20、针对受保护的资产和云安全组件进行自定义流量编排 21、IPv4/IPv6双栈：支持IPv4和IPv6双栈协议 22、系统维护：支持系统自动诊断检测，支持检测各项服务的状态 23、云安全组件订单管理：支持查看和管理所有云安全组件产品开通订单情况、状态，查看开通时间、账户、订单详情等 24、工单管理：查询和管理所有云租户工单 25、工单审批：审批所有云租户工单 26、访问管理：设置云安全资源池访问方式 27、认证策略：设置认证方式、双因子认证、用户密码强度等 28、登录安全策略：支持设置访问IP、超时锁定等策略 29、日志管理：支持设置日志记录策略、日志备份策略 30、短信联动：支持设置与常见短信网关联动 31、邮件联动：支持设置邮件服务器联动 32、升级管理：平台软件升级、升级历史查询 33、规则库升级管理：云安全组件规则库导入、一键升级、升级历史查询 34、用户管理：设置云安全资源池全局的超级管理员、安全管理员、审计管理员等；支持对用户进行创建、查询、删除、重置密码 35、角色管理：支持对所有用户角色进行自定义功能授权和角色分配 36、支持查看用户登录日志、系统日志等系统级日志 ▲37、支持安全组件分配功能，管理员可直接为各个云租户分配安全资源，同时完成关键安全资源的策略初始化。（提供产品功能截图并加盖厂商公章） ▲38、支持在系统界面上动态分配安全组件性能规格，允许对已分配组件规格进行动态变更和授权回收；回收的授权可分配至其他用户或其他类型安全组件。（提供产品功能截图并加盖厂商公章） ▲39、支持配置租户安全服务链：可灵活选择流量的源、目的以及途经的安全服务节点，并可调整节点的编排顺序。（提供产品功能截图并加盖厂商公章） ▲40、安全组件可独立于平台软件进行升级，快速获取最新功能；同时支持多租户组件批量升级，显著提升运维效率。（提供产品功能截图并加盖厂商公章）	项	1

1			2	云租户管理	1、威胁概览：支持展示近期发生的安全威胁的类型，每种安全威胁的时间变化趋势，可以查看最新安全威胁事件； 2、安全概览：支持查看当前已经开通的安全组件和攻击事件数量 3、威胁分析：风险总数、当日新增风险、高危风险、web安全事件、涉及资产数的统计展示 4、自定义报表：支持自定义报表 5、报表查询：支持按报表类型、日志、名称维度对报表进行查询 6、报表下载：支持报表下载 7、日志查询：支持查询和下载租户云安全产品日志 8、云安全组件申请：支持以工单形式申请云安全组件 9、云安全组件查询：支持查询已开通的云安全组件情况和状态 10、云安全组件退订：支持对已开通的云安全组件进行退订 11、云安全组件操作：支持对已开通的云安全组件进行部署操作，可单点登录到对应云安全组件；支持重启、停止、删除云安全组件实例 12、工单管理：支持对云租户单位内部工单管理、审批 13、信息管理：支持查看和管理云租户自身单位的云安全组件开通和使用情况 14、成员管理：支持创建和管理云租户自身单位账户 15、权限管理：支持对云租户自身单位账户权限的分配、管理、授权；支持对从功能模块、账户、资产、云安全组件等维护进行权限管理 16、订单管理：支持对云租户自身所有云安全组件订单进行管理、查询 17、日志管理：支持对云租户自身的所有操作日志、使用日志等管理和查询	项	1

3	云安全组件服务-漏洞扫描	1、管理可扫描的主机、数据库、Web站点等资产 2、对主机资产进行扫描，并进行漏洞管理 3、对Web站点资产进行扫描，并进行漏洞管理 4、对数据库资产进行扫描，并进行漏洞管理 5、对主机、数据库、中间件等进行核查，提供安全整改建议 6、对主机、数据库、Web应用等进行弱口令扫描，支持自定义用户名密码字典 7、对扫描的漏洞结果进行汇总统计、展示和导出 8、提供操作日志查询、统计、分析等	采用虚拟化技术，集成网络安全、数据安全等安全能力，为用户提供一站式云安全综合解决方案。以安全资源池的方式融合多种安全能力向用户进行一站式提供，支撑云内租户单位的独立安全管理，满足各上云单位的等级保护2.0安全需求，并支持通过管理平台进行统一调度、配置、监控和分析。支持租户管理；政务外网云安全资源池可支持35个上云业务单位通过等级保护2.0测评。	35
4	云安全组件服务-API审计	1、支持API接口流量审计和过滤 2、支持采集接口流量数据，支持状态监控和管理 3、支持对应用、API接口识别，可识别和划分接口类型及标签 4、支持对API接口账户的识别、提取 5、支持对API传输文件的审计、识别 6、支持API传输的常见敏感数据识别 7、支持API接口行为风险识别和预警 8、支持接口访问记录，并展示详情		
5	云安全组件服务-数据库审计	1、支持对可审计的数据库进行管理，支持国产数据库、关系型、大数据等常见数据库 2、支持审计数据库的操作类型、数据库账号、客户端IP、服务器IP、语句执行时间、返回结果等 3、支持对关于数据库的安全风险监测审计、预警，可对数据库风险操作行为、攻击行为进行告警 4、支持设置安全审计和风险监测策略，支持自定义策略 5、支持对审计数据进行多维报表统计和呈现		
6	云安全组件服务-日志审计	1、支持通过Syslog、SNMP、FTP等常见方式收集云主机资产日志 2、支持提供所采集日志数据的合规存储、查询回溯 3、支持对采集日志数据的综合统计、多维分析和呈现、导出 4、支持日志集中存储、备份、加密等策略管理 5、支持对提供日志数据的资产进行管理，支持对日志采集Agent进行管理，包括启动、停止、卸载、状态监控等		
7	云安全组件服务-主机安全	1、收集云主机所有资产信息和运行状况，包括进程、启动项、账户等详细信息 2、支持云主机防病毒，支持实时防护和主动扫描 3、支持对针对云主机的攻击行为进行防护 4、支持对黑客攻击行为进行检测，支持主机基线核查、主机风险自评估、主机账户异常行为等检测和预警，支持威胁情报匹配 5、支持主机安全日志的查询、统计、分析		
8	云安全组件服务-流量监测审计	1、支持配置安全监测策略，支持自定义策略 2、支持对流量采集进行管理，包括启动、停止、卸载、状态监控等 3、支持对常见攻击行为、恶意文件攻击行为进行检测 4、支持对攻击行为的多维查询、统计、回溯、分析		
9	云安全组件服务-Web防火墙	1、支持对保护的站点进行管理，可配置HTTP、HTTPS防护 2、支持对保护站点的跨站脚本(XSS)、注入式攻击、Webshell攻击、漏洞攻击、未授权访问等Web攻击行为防护 3、支持对常见敏感信息泄露行为进行防护，防止通过web获取服务器或后端敏感信息 4、支持基于规则的攻击防护策略，支持自定义策略 5、支持对防护日志的查询、统计、分析 6、支持记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容、cookie等内容		
10	云安全资源池定制	定制费用，含可视化展示、与态势感知平台对接、与云平台对接、接口开发定制、根据现状适配优化功能等。	项	1
11	维保	提供三年云安全资源池原厂维保服务。	项	1

标的名称：系统集成		12	交换机	接入交换机，支持堆叠，支持IPv6；≥48个10GE光口（按需配置光模块），≥6个40GE光口（按需配置光模块），AC冗余电源；交换容量≥2.16Tbps，包转发率≥1071Mpps；提供三年原厂质保及硬件维保服务。	台	2

序号	参数性质	技术参数与性能指标
1		包含安全设备、平台、服务等安装实施、系统联调测试、系统集成交付，包括系统集成范围内的辅材采购、技术服务等。

3.4商务要求

3.4.1交货时间

采购包1:

自合同签订之日起150个日历天内完成全部货物供应和安装调试工作并具备验收条件

3.4.2交货地点

采购包1:

采购方指定地点

3.4.3支付方式

采购包1:

分期付款

3.4.4支付约定

采购包1:

1、 预付款，合同正式签订后、供应商提供合法有效等额增值税发票，达到付款条件起15个工作日内，支付合同总金额的40.0%

2、 进度款，产品全部到货，开箱验收合格并具备安装条件，供应商提供合法有效等额增值税发票，达到付款条件起15个工作日内，支付合同总金额的30.0%

3、 进度款，安装部署完成、系统正常运行、功能满足采购需求，双方签署初步验收报告，供应商提供合法有效等额增值税发票，达到付款条件起15个工作日内，支付合同总金额的20.0%

4、 进度款，系统、设备连续稳定运行30天无故障，双方签署最终验收报告，供应商提供合法有效等额增值税发票，达到付款条件起15个工作日内，支付合同总金额的10.0%

3.4.5验收标准和方法

采购包1:

按国家及行业标准、采购需求、投标文件、合同约定执行，实行开箱验收、初步验收、最终验收三级验收，验收须形成书面验收报告。

3.4.6包装方式及运输

采购包1:

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7质量保修范围和保修期

采购包1:

中标供应商应当保证所供货物的来源渠道正常，产品是全新的、未使用过的，且完全符合合同规定的质量、规格、技术指标等要求，并对由于产品设计、工艺或材料的缺陷而产生的质量问题负责。维修响应：质保期内设备自身故障、系统问题，中标供应商提供原厂免费维修、更换配件及上门服务；逾期，采购人直接委托第三方处理，相关费用由中标供应商承担。超出质保期且需要更换配件的，中标供应商按市场最低价提供合格配件，免费安装维修。

3.4.8违约责任与解决争议的方法

采购包1:

根据合同条款约定。

3.5其他要求

供应商为法人分支机构（分公司）参与本项目投标的，须同时提供以下资料，缺一项则资格审查不通过：（1）分公司营业执照；（2）法人（负责人）给分支机构出具的授权书；需加盖公章。

第四章 资格审查

资格审查由采购人或代理机构组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

资格审查标准及要求如下:

4.1一般资格审查

采购包1:

序号	审查内容	具体标准和要求	关联投标（响应）文件格式文件
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料;	关于财务会计制度的证明材料｛注：①可提供2025年度经审计的财务报告（财务审计报告需附带财政部注册会计师行业统一监管平台备案的二维码及报告编码、在财政部注册会计师行业统一监管平台可查询，报告内容需包含审计报告和审计报告中所涉及的财务报表和报表附注）及财务情况说明书，②可提供文件递交截止日前三个月内从基本户银行开具的资信证明。提供二者任意一项即可｝;供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
3	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； 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，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函

4.2特殊资格审查

采购包1:

序号	审查内容	具体标准和要求	关联投标（响应）文件格式文件
1	主体资格	供应商应为具有独立承担民事责任能力的法人、其他组织或自然人，并出具合法有效的营业执照或事业单位法人证书等国家规定的相关证明，自然人参与的提供其身份证明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
2	税收缴纳证明	提供文件递交截止日前六个月内任意1个月的纳税证明或完税证明，相关证明材料，证明资料上应有相关机构的公章或业务专用章。依法免税的投标人应提供相关文件证明;供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
3	社会保障资金缴纳证明	提供文件递交截止日前六个月内任意1个月的社会保障资金相关证明材料，证明资料上应有相关机构的公章或业务专用章。依法不需要缴纳社会保障资金的投标人应提供相关文件证明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料

4	承诺函	提供具有履行合同所必需的设备和专业技术能力的承诺函；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
5	信誉要求	供应商不得为“信用中国”中列入失信被执行人和重大税收违法案件当事人名单的供应商，不得为“中国政府采购网”政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商，提供截图和承诺书。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章	投标人应提交的相关资格证明材料
6	授权代表	提供法定代表人授权书（附有效的法定代表人、被授权人身份证复印件）；法定代表人直接参加投标的，只须提供法定代表人身份证明文件；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	法人授权书.docx 法人证明书.docx 投标人应提交的相关资格证明材料
7	无违法记录证明	供应商出具本企业参加政府采购活动前三年内经营活动中没有重大违法记录的书面声明。供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
8	不接受联合体投标	提供非联合体声明；供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料

4.3落实政府采购政策资格审查

采购包1:

序号	**审查内容**	**具体标准和要求**	**关联投标（响应）文件格式文件**
无			

第五章 评标办法

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》《政府采购货物和服务招标投标管理办法》《陕西省政府采购评审专家管理实施办法》等法律规章，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序和标准对待所有的投标人。

四、本项目采取电子评标，通过项目电子化交易系统完成评标工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标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标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人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，评标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、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；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标活动的，将依法追究其责任。

5.2评标委员会

一、评审专家是采取随机方式在政府采购平台的专家库系统（以下简称专家库系统）抽取/由采购人根据《陕西省政府采购评审专家管理实施办法》（陕财办采〔2018〕20号）的规定，报主管部门同意后自行选定。

二、评标委员会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、推荐评标委员会组长。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；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投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

（一）熟悉和理解招标文件；

（二）审查供应商投标文件等是否满足招标文件要求，并作出评价；

（三）根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出澄清、说明或者更正；

（四）推荐中标候选供应商，或者受采购人委托确定中标供应商；

（五）起草评标报告并进行签署；

（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 评标方法

采购包1：综合评分法

5.4评标程序

5.4.1熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项目技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

（一）招标文件的规定存在歧义、重大缺陷的；

（二）招标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，但是招标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，但是招标文件未依法体现促进中小企业发展相关规定的；

（五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；

（六）招标文件将投标人的资格条件列为评分因素的；

（七）招标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标情形的，评标委员会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，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，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，同时在陕西省政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，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。

5.4.2符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会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招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

采购包1:

序号	审查内容	具体标准和要求	关联投标（响应）文件格式文件
1	不正当竞争预防措施（实质性要求）	1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在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，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、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.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会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。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。	开标一览表 标的清单
2	签名、盖章	投标人必须按照招标文件的规定和要求在投标文件中指定的页面落款处加盖公章并由法定代表人或被授权人签名（或盖章），其余页面逐页盖公章，否则将作为无效投标文件处理。招标文件凡是要求法定代表人签名或盖章之处，非法人单位的负责人均参照执行。	本国产品说明.docx 法人证明书.docx 中小企业声明函 商务应答表 投标人应提交的相关资格证明材料 法人授权书.docx 产品技术参数表 投标函 残疾人福利性单位声明函 项目方案.docx 供应商项目业绩一览表.docx 标的清单 关于符合本国产品标准的声明函 投标文件封面 陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书.docx 监狱企业的证明文件
3	报价	投标文件所有报价未超过最高限价	标的清单
4	其他	1、供应商针对同一项目递交两份或多份内容不同的响应文件，未书面声明哪一份是有效的或出现选择性报价的； 2、提供虚假资料；提供虚假资质、虚假技术 指标证明材料、虚假证明（包括第三方提供的虚假证明）；出现虚假应答、承诺、声明的； 3、供应商附加了采购单位难以接受的条件或条款的； 4、供应商前期参与了本次项目方案设计的；5、在政府采购或其它重大项目履约过程中有不良记录或未能按期履约的；6、供应商使用虚假印章或印章无法证实为真实有效； 7、响应文件的关键内容字迹模糊、无法辨认的； 8、不符合法律、法规规定的其它实质性要求的。	本国产品说明.docx 法人证明书.docx 中小企业声明函 商务应答表 投标人应提交的相关资格证明材料 法人授权书.docx 产品技术参数表 投标函 残疾人福利性单位声明函 项目方案.docx 供应商项目业绩一览表.docx 标的清单 关于符合本国产品标准的声明函 投标文件封面 陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书.docx 监狱企业的证明文件

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员

会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标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招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

（一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；

（二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料；

（三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

（一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

（二）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；

（三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；

（四）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。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评价。

5.4.5复核

评标结果汇总完成后、评审报告签署前，采购人及代理机构应严格依照《财政部关于印发<政府采购竞争性磋商采购方式管理暂行办法>的通知》《政府采购货物和服务招标投标管理办法（财政部令第87号）》《政府采购非招标采购方式管理办法（财政部令第74号）》及《陕西省财政厅关于规范政府采购项目评审主观分赋分有关事项的通知》（陕财办函〔2026〕10号）等文件要求，对评审数据进行全面校对与核对，重点核查各评审专家主观分项评分与全体评委对应分项平均分的偏离情况，确保评审数据准确无误、流程合规。

5.4.6确定中标候选人名单

采购包1： 按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

一、招标公告刊登的媒体名称、开标日期和地点；

二、投标人名单和评标委员会成员名单；

三、评审方法和标准；

四、开标记录和评审情况及说明，包括投标无效供应商名单及原因；

五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人；

六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者补正，评标委员会成员的更换等；

七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理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，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，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。

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

若采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。 投标报价得分=（评标基准价／投标报价）×100

评标总得分＝F1×A1＋F2×A2＋……＋Fn×An

F1、F2……Fn分别为各项评审因素的得分；

A1、A2、……An 分别为各项评审因素所占的权重（A1＋A2＋……＋An＝1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2评分标准

采购包1:

评审内容		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	评审内容	具体标准和要求	分值	客观/主观	关联投标（响应）文件格式文件
	产品响应	1.标注“★”的技术指标共1项为实质性响应条款，供应商未响应、响应不满足要求的，其投标作无效投标处理。 2.标注“▲”的重要技术指标共37项，本项满分37分，每项对应分值1分；每出现1项负偏离扣1分，扣完本项37分为止。 3.除上述★、▲类指标外，其余为一般技术指标，供应商须逐条逐项列明响应情况，并按要求提供佐证材料。供应商须在《产品技术参数表》中对应标注佐证材料页码，并在佐证材料对应参数位置醒目标注，由评标委员会核查响应真实性及材料有效性。投标人存在一般技术指标负偏离的，不做否决投标、不扣减评审得分，但该偏离情况将如实记入评标报告及合同附件，中标人应按招标文件要求完成供货及服务；履约验收如达不到招标文件一般参数要求，按合同约定承担违约责任。 注：佐证材料要求：（1）“★”、“▲”指标提供佐证材料包括但不限于产品彩页、官网截图（含网址及截图时间）、合格证书、第三方检测报告、认证证书等；（2）一般指标提供佐证材料包括但不限于产品彩页、官网截图（含网址及截图时间）、合格证书、第三方检测报告、认证证书、生产厂商盖单位公章的参数确认函、售后承诺函等。	37.0000	客观	产品技术参数表

详细评审	实施方案	提供针对本项目的实施方案。包括但不限于（1）供货、安装调试；（2）实施步骤、进度计划和保证措施；（3）项目实施安全控制方案；（4）质量保障措施。方案各项内容全面详细、阐述条理清晰、技术先进、功能配置合理，能有效保障本项目实施得8分，每有一项缺项扣2分，每项内容有一处存在缺陷，扣1分，扣完为止。（备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施；）	8.0000	主观	项目方案.docx
	供货组织安排	供货组织安排：投标人针对本次招标任务有具体的供货组织安排，包括但不限于（1）供货周期管控；（2）物流与交付保障方案；各部分内容全面详细、阐述条理清晰详尽、符合本项目采购需求得3分；评审内容每缺一项扣1.5分；每项内容有一处存在缺陷，扣0.5分，扣完为止（缺陷是指：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。）	3.0000	主观	项目方案.docx
	技术培训方案	具有可行的技术培训方案，保证使用单位能熟练操作维护和正常使用，列出详细的（1）培训计划；（2）培训内容；（3）培训形式和目标等说明；方案各项内容全面详细、阐述条理清晰、切实可行，能有效保障本项目实施得3分，每有一项缺项扣1分，每项内容有一处存在缺陷，扣0.5分，扣完为止。（备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。）	3.0000	主观	项目方案.docx
	应急保障及售后服务方案	供应商针对本项目提供完善合理的应急保障及售后服务。包括但不限于（1）进度延误；（2）出现质量问题时的补救措施；（3）售后服务计划；（4）售后服务措施；（5）服务人员保障及故障响应时间；（6）售后服务承诺。方案各项内容全面详细、阐述条理清晰、切实可行、功能配置合理，能有效保障本项目实施得6分，每有一项缺项扣1分，每项内容有一处存在缺陷，扣0.5分，扣完为止。（备注：缺陷是指内容不合理、虽有内容但不完善、内容表述前后不一致、套用其他项目方案或与项目需求不匹配及其他不利于项目实施的等任意一种情形。）	6.0000	主观	项目方案.docx

业绩	提供2024年9月1日以来类似项目业绩（以合同签订日期为准）的业绩证明文件（每个项目业绩需提供完整合同、中标通知书二者缺一不可），评审时以业绩证明文件的扫描件为计分依据，每提供一份业绩证明文件得2分，满分4分。（注：类似业绩指的是包含网络安全设备的政府采购项目）	4.0000	客观	供应商项目业绩一览表.docx
人员配备	供应商有完善的项目管理方案，整个项目设有项目经理人及其他等有关人员，提供人员组织架构清单。1、项目经理持有计算机技术与软件专业技术资格信息系统项目管理师（高级）得4分；或持有计算机技术与软件专业技术资格系统集成项目管理工程师（中级）得2分 、项目经理须完整提供学历证书、资格证书，身份证，近三个月任意1个月本单位社保缴纳证明或劳动合同，不提供或少提供相关证明文件不得分。 2、其他人员要求：除项目经理外，另行配备5名具备相关资格证书的人员，每名人员均须完整提供身份证、学历证书、资格证书、近三个月任意1个月本单位社保证明或劳动合同；提供一人得1分，满分5分，不提供或少提供每人相关证明文件的不得分。	9.0000	客观	项目方案.docx

异常低价审查	异常低价审查	根据《关于推动解决政府采购异常低价问题的通知》（财库〔2026〕2号）等相关规定，政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序： （1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值65%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×65%。 （2）投标（响应）报价低于通过符合性审查且报价次低供应商投标（响应）报价65%的，即投标（响应）报价<通过符合性审查且报价次低供应商投标（响应）报价×65%。 （3）投标（响应）报价低于最高限价65%的，即投标（响应）报价<最高限价×65%。 （4）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价（数量报价下，投标人的报价明显高于其他通过符合性审查投标人的报价），有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。 评审委员会启动异常低价投标（响应）审查后，应当要求相关供应商在评审现场合理的时间内提供书面说明及必要的证明材料，对投标（响应）价格作出解释。	0.0000	客观	开标一览表 标的清单
价格分	价格分	经资格审查、符合性审查合格的投标响应文件，其投标报价为有效投标报价。满足投标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。价格分按照下列公式计算。 投标报价得分=(评标基准价／投标报价)×30	30.0000	客观	开标一览表 标的清单 关于符合本国产品标准的声明函 本国产品说明.docx

价格扣除

序号	**价格扣除评审内容**	**适用情形**	**扣除比例（C1）**	**具体标准和要求**	**关联投标（响应）文件格式文件**

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 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
2	实施本国产品标准	本国产品标准适用于货物，包括政府采购货物项目和服务项目中涉及的货物。适用本国产品标准的货物具体是指《政府采购品目分类目录》中的货物类产品，但不包括其中的房屋和构筑物，文物和陈列品，图书和档案，特种动植物，农林牧渔业产品，矿与矿物，电力、城市燃气、蒸汽和热水、水，食品、饮料和烟草原料，无形资产	20.00%	政府采购活动中既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予20%的价格扣除，用扣除后的价格参与评审。当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予20%的价格扣除，用扣除后的价格参与评审	关于符合本国产品标准的声明函 本国产品说明.docx 标的清单

说明:

1、评分的取值按四舍五入法，保留小数点后两位;

2、评分标准中要求提供复印件的证明材料须清晰可辨。

若采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标:

一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的;

二、出现影响采购公正的违法、违规行为的;

三、投标人的报价均超过了采购预算，采购人不能支付的;

四、因重大变故，采购任务取消的。

废标后，代理机构将在“陕西省政府采购网”上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定1名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

5.8.2定标程序

一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起2个工作日内将评标报告送采购人。

三、采购人在收到评标报告后5个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在陕西省政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9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。

5.10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，不得修改或细化采购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，除因配合答复处理供应商的询问、质疑和投诉等事项外，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 投标文件格式

采购包1:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

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：投标人应提交的相关资格证明材料

详见附件：产品技术参数表

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：关于符合本国产品标准的声明函

详见附件：本国产品说明.docx

详见附件：法人证明书.docx

详见附件：法人授权书.docx

详见附件：供应商项目业绩一览表.docx

详见附件：陕西省政府采购供应商拒绝政府采购领域商业贿赂承诺书.docx

详见附件：项目方案.docx

第七章 拟签订采购合同文本

详见附件：铜川市政务云平台安全能力提升建设项目合同模版.docx