

招 标 文 件

(服务类)

采购项目名称: **2025年西安市市级政务信息化公共基础平台一体化安全服务项目**

采购项目编号: **SNJZ-2025-122**

西安市数据局

陕西教育招标有限责任公司共同编制

2025年06月17日

第一章 投标邀请

陕西教育招标有限责任公司（以下简称“代理机构”）受西安市数据局委托，拟对**2025年西安市市级政务信息化公共基础平台一体化安全服务项目**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：**SNJZ-2025-122**

二、采购项目名称：**2025年西安市市级政务信息化公共基础平台一体化安全服务项目**

三、招标项目简介

本项目采取购买服务的方式，采购安全管理体系服务、基础安全防护服务、统一安全运维服务。

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：

落实政府采购促进中小企业发展的相关政策：

采购包2（监理服务）：属于专门面向中小企业采购。

（三）本项目的特定资格要求：

采购包1：

1、营业执照：具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。

2、法人代表授权书：法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。

3、财务状况报告：法人提供经审计的**2023年度或2024年度**的财务报告或提交投标文件递交截止时间前一年内银行出具的资信证明；其他组织和自然人提供银行出具的资信证明或财务报表；或政府采购信用担保机构出具的《政府采购投标担保函》。

4、税收缴纳证明：提供投标文件递交截止时间前近一年内至少一个月已缴纳的纳税凭据或完税证明；依法免税的供应商应提供相关文件证明。

5、社会保障资金缴纳证明：提供投标文件截止时间前近一年内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

6、具有履行本合同所必需的设备和专业技术能力：提供具有履行本合同所必需的设备和专业技术能力的承诺书。

7、政府采购活动前三年内在经营活动中没有重大违法记录：提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。

采购包2：

1、营业执照：具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。

2、法人代表授权书：法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。

3、财务状况报告：法人提供经审计的**2023年度或2024年度**的财务报告或提交投标文件递交截止时间前一年内银行出具的资信证明；其他组织和自然人提供银行出具的资信证明或财务报表；或政府采购信用担保机构出具的《政府采购投标担保函》。

4、税收缴纳证明：提供投标文件递交截止时间前近一年内至少一个月已缴纳的纳税凭据或完税证明；依法免税的供应商

应提供相关文件证明。

5、社会保障资金缴纳证明：提供投标文件截止时间前近一年内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。

6、具有履行本合同所必需的设备和专业技术能力：提供具有履行本合同所必需的设备和专业技术能力的承诺书。

7、政府采购活动前三年内在经营活动中没有重大违法记录：提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。

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（<http://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登录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：

在线客服：通过陕西省政府采购网-在线客服进行咨询

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及签章服务进行查询

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。

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、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录陕西省政府采购网—陕西省政府采购金融服务平台（<http://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：西安市数据局

地址：西安市未央区凤城八路109号

邮编：710007

联系人：张老师

联系电话：029-86788399

代理机构：陕西教育招标有限责任公司

地址：西安市雁塔区太白南路181号西部电子社区A座B区401

邮编：710065

联系人：崔斌、程钰、马子啸、王力

联系电话：029-88224929

采购监督机构：西安市财政局政府采购管理处

联系人：杜新星

联系电话：029-89821846

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）	<p>本项目各包采购预算金额如下：</p> <p>采购包1：14,127,864.00元</p> <p>采购包2：224,886.00元</p> <p>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。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>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。</p>
3	评标方法	<p>采购包1：综合评分法</p> <p>采购包2：综合评分法</p> <p>（详见第五章）</p>
4	是否接受联合体	<p>采购包1：不接受</p> <p>采购包2：不接受</p> <p>如以联合体响应的，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。</p> <p>（1）联合体各方均应具有承担本项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）招标文件对投标人资格条件有特殊要求的，联合体各个成员都应当具备规定的相应资格条件。</p> <p>（3）同一专业的单位组成的联合体，应当按照资质等级较低的单位确定联合体的资质等级。如：某联合体由三个单位组成，其中两个单位资质等级为甲级，另一单位资质等级为乙级，则该联合体资质等级等级为乙级。</p>
5	落实节能、环保产品政策	<p>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。</p> <p>2.本项目采购若有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。</p> <p>3.本项目采购若有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，本项目采购若有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。</p>

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	充分、公平竞争保障措施（实质性要求）	<p>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。</p> <p>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。</p> <p>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。</p> <p>核心产品清单详见第三章。</p> <p>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。</p>
8	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。
9	投标保证金	缴交方式：否
10	标书费信息	免费获取
11	履约保证金（实质性要求）	<p>采购包1：不缴纳</p> <p>采购包2：不缴纳</p>
12	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。
13	招标代理服务费（实质性要求）	<p>本项目收取代理服务费</p> <p>代理服务费用收取对象：中标/成交供应商</p> <p>代理服务费收费标准：定额收取 采购包1：39000.00元 采购包2：1000.00元 开户行：中国光大银行陕西自贸试验区西安唐延路支行 开户名称：陕西教育招标有限责任公司 银行行号：303791000136 开户账号：78580188000058925 财务电话：029-88224928</p>
14	采购结果公告	采购结果将在陕西省政府采购网予以公告。
15	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。

16	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，采购人将政府采购合同报本级财政部门备案。
17	进口产品	不允许
18	是否组织潜在投标人现场考察	采购包1：组织现场踏勘：否 采购包2：组织现场踏勘：否
19	特殊情况	出现下列情形之一的，采购人或者代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。 （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，采购人或者采购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，采购人或者采购代理机构应当依法废标。

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西安市数据局和陕西教育招标有限责任公司享有。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，评标细则及标准由西安市数据局负责解释。除上述招标文件内容，其他内容由陕西教育招标有限责任公司负责解释。

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西安市数据局。

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陕西教育招标有限责任公司。

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

三、如采用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）电子印章，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。

投标文件提交截止时间前30分钟，投标人登录项目电子化交易系统-“开标/开启大厅”参与开标。

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交易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、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个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。

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。

采购包2：不允许合同分包。

2.6.2.2 合同转包

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

二、中标供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3 采购人增加合同标的权利

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。

2.6.4 履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

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

2.6.5 履约验收方案

采购包1：

验收：投标人按照采购文件及合同内容提供完整服务，服务期满且无争议，考核合格，视为验收合格。验收过程中，若发现严重质量问题，且在规定时间内整改无效，采购人将进行严肃处理，并将其列入“不良行为记录名单”。验收依据 招标文件、投标文件、合同文本、国内相应的标准、规范。

采购包2：

验收：投标人按照采购文件及合同内容提供完整服务，服务期满且无争议，考核合格，视为验收合格。验收过程中，若发现严重质量问题，且在规定时间内整改无效，采购人将进行严肃处理，并将其列入“不良行为记录名单”。验收依据 招标文件、投标文件、合同文本、国内相应的标准、规范。

2.6.6 资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7 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）

投标人参加投标不得有下列情形：

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、未按照招标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，具有前述一至十三条情形之一的，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 陕西教育招标有限责任公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西教育招标有限责任公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西教育招标有限责任公司 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（包括但不限于文字错误、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）质疑函正本1份；（政府采购供应商质疑函范本详见附件一）
- （二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；
- （三）法定代表人或主要负责人身份证复印件1份；
- （四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；
- （五）针对质疑事项必要的证明材料（针对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：崔斌

联系电话：029-88224929

地址：西安市雁塔区西部电子社区A座B区401

邮编：710065

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招标文件、采购过程、采购结果的范围。

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

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

第三章 招标项目技术、服务、商务及其他要求

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

3.1采购项目概况

本项目采取购买服务的方式，采购安全管理体系服务、基础安全防护服务、统一安全运维服务以及监理服务。

3.2服务内容及服务要求

3.2.1服务内容

采购包1：
采购包预算金额（元）：14,127,864.00
采购包最高限价（元）：14,127,864.00
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
1	2025年西安市市级政务信息化公共基础平台一体化安全服务项目	1.00	14,127,864.00	项	软件和信息技术服务业	否	否	否	否

采购包2：
采购包预算金额（元）：224,886.00
采购包最高限价（元）：224,886.00
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
1	监理服务	1.00	224,886.00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：
标的名称：2025年西安市市级政务信息化公共基础平台一体化安全服务项目

序号	参数性质	技术参数与性能指标
		1.基础安全防护服务

序号	一级服务内容	二级服务内容	服务要求	服务支撑工具 / 设备数量	服务周期 (月)
1	防火墙服务	政务外网	<p>1.服务期内以防火墙为支撑工具/设备为政务外网广域网接入提供防火墙服务，基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略为政务外网广域网边界提供安全访问控制。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥ 6个，千兆光口≥ 12个，万兆SFP+接口≥ 8个，并根据实际业务组网需要配备接口光模块及跳线；整机吞吐量$\geq 80\text{Gbps}$，最大并发连接数≥ 1200万，每秒TCP新建连接数≥ 40万。</p> <p>2.支持透明、路由、混合、旁路等部署模式。</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。</p> <p>5.病毒库不少于140万种病毒特征。</p> <p>6.内置IPS特征库（至少应包括信息窃取、木马后门、间谍软件、可疑行为、网络设备攻击、安全漏洞及网络数据库攻击等的特征事件），特征规则数量不少于9000条，特征库可按分组进行管理。</p> <p>7.▲支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析。</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器。</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2
		广域网接入安全防护			

			服务	2	<p>1.服务期内以态势感知探针为支撑工具/设备对流经政务外网广域网区的网络流量进行实时检测，及时发现网络中存在的已知威胁和未知威胁流量，并给态势感知平台提供网络安全数据源服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥4个，千兆光口≥4个，万兆SFP+接口≥4个，RJ-45管理接口≥1个，USB 接口≥4个，内存≥128G，硬盘存储空间≥18T，并根据实际业务组网需要配备接口光模块及跳线；网络流量处理能力≥15Gbps，每秒新建连接数≥10万，最大并发连接数≥800万，应用层性能≥20Gbps。</p> <p>2.支持双向检测事件库≥20000个；</p> <p>3.▲支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书，对加密流量进行解密及还原；支持SSL3.0，TLS1.0/1.1/1.2；</p> <p>4.持基于工具特征的WEBSHELL检测:如冰蝎连接；</p> <p>5.支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识，告警结果呈现结果至少包多个维度：告警数据展示、基础数据展示、事件描述、云查情报、流量还原；</p> <p>6.支持通过syslog/kafka/SNMP trap方式将告警日志、违规互联日志、威胁情报日志、流数据日志、协议元数据外发至第三方数据采集平台，支持同时配置多个外发采集平台；</p>	1	1 2
			负载均衡服务	3	<p>1.服务期内以负载均衡为支撑工具/设备为凤八各行政办公园区、凤城十二路凯瑞大厦集中办公区、劳动南路集中办公区等区域内的各委办局政务外网计算机终端访问互联网提供负载均衡服务、包含NAT转换、路由转发、链路负载等服务；支撑工具/设备符合国产化要求，应配备冗余电源；千兆电口≥4个、千兆光口≥8个、万兆SFP+接口≥4个，SSD硬盘存储空间≥512G，并根据实际业务组网需要配备接口光模块及跳线；整机最大吞吐量 ≥80Gbps，每秒新建数≥55万。</p> <p>2.支持透明、路由、混合及单臂、三角传输模式部署</p> <p>3.应用路由：支持在线视频，P2P下载，视频会议等应用的检测识别，可将相应流量分配到期望的目标链路。</p> <p>4.链路负载均衡算法：支持轮询、加权轮询、最小连接数、加权最小连接数、源ip哈希、源ip+端口哈希、目的IP哈希、动态就近性、最小流量、最小延时、最小抖动、最小丢包率、带宽比例、带宽剩余率等链路负载均衡算法；</p> <p>5.支持手动、自动创建系统快照，可在系统异常时，快速恢复正常的系统版本及配置。</p> <p>6.支持服务器负载大屏展示，包括VS基本信息、状态、流量、服务器成员质量、以及压缩和缓存等数据展示；</p> <p>7.为降低支撑工具/设备割接对现有业务的影响，提供现有负载均衡策略配置批量迁移导入方案。</p>	2	1 2

			互联网行政办公区安全防护服务	4	<p>上网行为管理服务</p> <p>1.服务期内以上网行为管理系统为支撑工具/设备为市各委办局政务外网计算机终端访问互联网提供上网行为管理、应用控制、行为审计、网络业务优化等服务。支撑工具/设备符合国产化要求，应配备冗余电源，最大支持带宽≥20G，管理口≥2个，千兆电口≥8个、千兆光口≥8个、万兆SFP+接口≥4个，硬盘存储空间≥4T，并根据实际业务组网需要配备接口光模块及跳线。HTTP吞吐量≥80Gbps，每秒新建连接数≥140万，最大并发连接数≥6000万。</p> <p>2.支持路由模式、透明（网桥）模式、混合模式、旁路模式；</p> <p>3.支持超过7000+的应用，支持超过5500+的种海外应用，并保持定期更新；</p> <p>4.支持通道化的QoS，支持基于用户、原地址、目的地址、应用、源/目的地址、地理位置、时间、终端型号进行带宽控制。</p> <p>5.支持针对搜索引擎、http、网页内容进行关键字过滤并实时生成日志记录，并支持将日志记录通过syslog等方式推送至态势感知平台。日志级别包括但不限于紧急、告警、严重、通知、信息、调试、不记录等。</p>	2	1 2
				5	<p>防火墙服务</p> <p>1.服务期内以防火墙为支撑工具/设备为市各委办局政务外网计算机终端访问互联网提供入侵防御、防病毒、URL控制和流量控制以及基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略服务。支撑工具/设备符合国产化要求，应配备冗余电源；千兆电口≥7个，千兆光口≥4个,万兆SFP+接口≥8个，并根据实际业务组网需要配备接口光模块及跳线； SSD硬盘存储空间≥256G，机械硬盘存储空间≥4T；整机吞吐≥80Gbps，TCP新建连接数≥800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式。</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护。</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。</p> <p>5.病毒库不少于140万种病毒特征。</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理。</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析。</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2

		6	负 载 均 衡 服 务	<p>1.服务期内以负载均衡为支撑工具/设备为互联网业务发布区提供负载均衡服务、包含NAT转换、路由转发、链路负载等服务；支撑工具/设备符合国产化要求，应配备冗余电源；千兆电口≥4个、千兆光口≥8个、万兆SFP+接口≥4个，SSD硬盘存储空间≥512G，并根据实际业务组网需要配备接口光模块及跳线；整机最大吞吐量 ≥80Gbps，每秒新建数≥55万。</p> <p>2.支持透明、路由、混合及单臂、三角传输模式部署</p> <p>3.应用路由：支持在线视频，P2P下载，视频会议等应用的检测识别，可将相应流量分配到期望的目标链路。</p> <p>4.链路负载均衡算法：支持轮询、加权轮询、最小连接数、加权最小连接数、源ip哈希、源ip+端口哈希、目的IP哈希、动态就近性、最小流量、最小延时、最小抖动、最小丢包率、带宽比例、带宽剩余率等链路负载均衡算法；</p> <p>5.支持手动、自动创建系统快照，可在系统异常时，快速恢复正常的系统版本及配置。</p> <p>6.支持服务器负载大屏展示，包括VS基本信息、状态、流量、服务器成员质量、以及压缩和缓存等数据展示；</p> <p>7.为降低支撑工具/设备割接对现有业务的影响，提供现有负载均衡策略配置批量迁移导入方案。</p>	2	1 2
		7	运 营 商 级 抗 D D o S 服 务	<p>1.服务期内为招标人互联网业务发布区提供运营商机抗DDoS防护服务，提供5G不限次数防护服务；</p> <p>2.十二个月协议期内提供≥6 次 5G 以上 100Gbps以下DDos 攻击防护服务；</p> <p>3.防护IP地址64个以内；DNS 解析不做变更，用户端零操作；</p> <p>4.提供抗DDoS服务区到采购方的服务器区≥1G的专用网络。</p>	2	1 2
			互 联 网 业 务 发 布			

			区 安 全 防 护 服 务	8	<p>抗 D D o S</p> <p>1.服务期内以抗DDoS为支撑工具/设备，基于DPI、DFI技术对互联网出口网络流量中不同的flow协议，网络应用层载荷进行深度检测，当检测DDoS攻击后，将异常流量进行清洗。支撑工具/设备符合国产化要求，应配备冗余双电源，整机抗攻击能力≥10Gbps，管理口≥2个，千兆电口≥4个（带2组bypass），千兆光口≥4个，万兆SFP+接口≥6个，并根据实际业务组网需要配备接口光模块及跳线；支持SYN/SYNACK/ACK Flood攻击、UDP Flood攻击、ICMP Flood等流量型攻击和DNS query flood攻击、CC攻击、HTTP get flood攻击、Connection flood等应用型攻击。</p> <p>2.支持自动防护，系统开启自动防护后，无需撰写任何规则对所有服务器进行DDoS防护，也可针对特定服务器撰写特定防护规则；</p> <p>3.支持根据国家/地区（国内精确到省份）进行拦截、放行、防护、限速等策略，支持手动导入GeoIP库，支持联网自动更新GeoIP库，显示更新状态；</p> <p>4.支持双向流量控制，支持设置入方向和出方向的总流量，TCP流量、UDP流量、FRAG流量、ICMP流量以及其他协议的阈值对双向流量限制。粒度可控制到单个IP，也支持整机限制；</p> <p>5.支持创建系统镜像，该镜像包括系统软件及全量配置信息，并可以回退到指定镜像文件，支持不少于8个镜像文件；</p>	2	1 2
				9	<p>防 火 墙 服 务</p> <p>1.服务期内以防火墙为支撑工具/设备为互联网发布业务提供基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥7个，千兆光口≥4个，万兆SFP+接口≥16个，40G万兆QSFP接口≥2个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间≥256G，机械硬盘存储空间≥4T；防火墙吞吐≥160Gbps，最大并发连接数≥2000万，TCP新建连接数≥800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式；</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护。</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。</p> <p>5.病毒库不少于140万种病毒特征；</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理；</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2

1 0	局域网区（市政府、市委	防火墙服务	<p>1.服务期内以防火墙为支撑工具/设备，基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略为政务外网局域网边界提供安全访问控制服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥ 7个，千兆光口≥ 4个,万兆SFP+接口≥ 8个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间$\geq 256G$，机械硬盘存储空间$\geq 4T$；整机吞吐$\geq 80Gbps$，最大并发连接数≥ 2000万，TCP新建连接数≥ 800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式；</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护；</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式；</p> <p>5.病毒库不少于140万种病毒特征；</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理；</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	6	1 2
	、综合楼）安全防护服务	态势感知探针服务	<p>1.服务期内以态势感知探针为支撑工具/设备对流经政务外网局域网边界的网络流量进行实时检测，及时发现网络中存在的已知威胁和未知威胁流量，并给态势感知平台提供网络安全数据源服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥ 4个，千兆光口≥ 4个，万兆SFP+接口≥ 4个，RJ-45管理接口≥ 1个，USB接口≥ 4个，内存$\geq 128G$，硬盘存储空间$\geq 18T$，并根据实际业务组网需要配备接口光模块及跳线；网络流量处理能力$\geq 15Gbps$，每秒新建连接数≥ 10万，最大并发连接数≥ 800万，应用层性能$\geq 20Gbps$。</p> <p>2.支持双向检测事件库≥ 20000个；</p> <p>3.支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书，对加密流量进行解密及还原；支持SSL3.0，TLS1.0/1.1/1.2；</p> <p>4.持基于工具特征的WEBSHELL检测:如冰蝎连接；</p> <p>5.支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识，告警结果呈现结果至少包多个维度：告警数据展示、基础数据展示、事件描述、云查情报、流量还原；</p> <p>6.支持通过syslog/kafka/SNMP trap方式将告警日志、违规互联日志、威胁情报日志、流数据日志、协议元数据外发至第三方数据采集平台，支持同时配置多个外发采集平台；</p>	1	1 2

1 2	政务云 平台 (凤 八 墙) 安 全 防 护 服 务	<p>1.服务期内以防火墙为支撑工具/设备为凤八政务云平台节点提供基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥7个，千兆光口≥4个,万兆SFP+接口≥16个，40G万兆QSFP接口≥2个，并根据实际业务组网需要配备接口光模块及跳线； SSD硬盘存储空间≥256G，机械硬盘存储空间≥4T；防火墙吞吐≥160Gbps，最大并发连接数≥2000万，TCP新建连接数≥800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式；</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护。</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。</p> <p>5.病毒库不少于140万种病毒特征；</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理；</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2
1 3	政务云 平台 (西 咸) 政 务 外 网 侧 安 全 防 护 服 务	<p>1.服务期内以防火墙为支撑工具/设备为西咸政务云平台节点提供基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥7个，千兆光口≥4个,万兆SFP+接口≥16个，40G万兆QSFP接口≥2个，并根据实际业务组网需要配备接口光模块及跳线； SSD硬盘存储空间≥256G，机械硬盘存储空间≥4T；防火墙吞吐≥160Gbps，最大并发连接数≥2000万，TCP新建连接数≥800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式；</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护。</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。</p> <p>5.病毒库不少于140万种病毒特征；</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理；</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2

			1 4	交 换 机 服 务	服务期内以交换机为支撑工具/设备为西咸政务云平台互联网出口提供专线接入服务。支撑工具/设备为标准1U机箱，配置≥24个千兆光口，≥4个万兆光口，并根据实际业务组网需要配备接口光模块及跳线；包交换容量≥64Gpps，支持端口聚合、镜像、VLAN、STP、MAC地址绑定， Qin Q等功能。	2	1 2
			1 5	防 火 墙 服 务	<p>1.服务期内以防火墙为支撑工具/设备，基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略为西咸政务云节点互联网出口提供安全访问控制服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥7个，千兆光口≥4个,万兆SFP+接口≥8个，并根据实际业务组网需要配备接口光模块及跳线；S SD硬盘存储空间≥256G ，机械硬盘存储空间≥4T；整机吞吐≥80Gbps ，最大并发连接数≥2000万，TCP新建连接数≥800万/秒。</p> <p>2.支持透明、路由、混合、旁路等部署模式；</p> <p>3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护；</p> <p>4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式；</p> <p>5.病毒库不少于140万种病毒特征；</p> <p>6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理；</p> <p>7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析；</p> <p>8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器；</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2

16	抗DDoS服务	<p>1.服务期内以抗DDoS系统为支撑工具/设备，基于DPI、DFI技术对西咸政务云节点互联网出口网络流量中不同的flow协议，网络应用层载荷进行深度检测，当检测DDoS攻击后，将异常流量进行清洗。支撑工具/设备符合国产化要求，应配备冗余电源，整机抗攻击能力≥2Gbps，管理口≥2个，千兆电口≥4个，千兆光口≥4个，万兆SFP+接口≥4个，并根据实际业务组网需要配备接口光模块及跳线。支持SYN/SYNACK/ACK Flood 攻击、UDP Flood 攻击、ICMP Flood等流量型攻击和DNS query flood攻击、CC攻击、HTTP get flood攻击、Connection flood等应用型攻击。</p> <p>2.支持自动防护，系统开启自动防护后，无需撰写任何规则对所有服务器进行DDoS防护，也可针对特定服务器撰写特定防护规则；</p> <p>3.支持根据国家/地区（国内精确到省份）进行拦截、放行、防护、限速等策略，支持手动导入GeolIP库，支持联网自动更新GeolIP库，显示更新状态；</p> <p>4.支持双向流量控制，支持设置入方向和出方向的总流量，TCP流量、UDP流量、FRAG流量、ICMP流量以及其他协议的阈值对双向流量限制。粒度可控制到单个IP，也支持整机限制；</p> <p>5.支持创建系统镜像，该镜像包括系统软件及全量配置信息，并可以回退到指定镜像文件，支持不少于8个镜像文件；</p>	2	12

[illegible]

18	全流量分析服务	<p>1.服务期内以全流量分析系统为支撑工具/设备，实时捕获并保存政务外网数据包，采集内容包括L2-L7层网络流量数据包；可将接收的流量实时转发，流量复制接口支持Web页面灵活设置，支持一进一出、一进多出、多进一出、多进多出的流量复制分发能力；支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥ 2个，千兆光口≥ 4个，并根据实际业务组网需要配备接口光模块及跳线；内存$\geq 64G$；网络流量处理能力$\geq 1Gbps$，每秒新建连接数≥ 2万，最大并发连接数≥ 100万，数据检索速度$\geq 50TB/秒$。</p> <p>2.存储硬盘不少于20T；</p> <p>3.支持存储过滤功能，支持配置报文只解析不存储策略规则，可查看到对应解析会话日志，无法下载对应报文；</p> <p>4.支持文件还原，可支持HTTP、FTP、邮件等协议文件还原提取MD5功能；</p> <p>5.支持资产关联分析，可对任意资产地址进行回溯关联，通过点状图可视化呈现资产连接情况，快速判断访问路径；</p> <p>6.支持原始数据包重放，可灵活选择需要回放的数据包，回放条件支持起止时间、BPF语法过滤规则、基于流的六元组过滤规则（源IP、目的IP、源端口、目的端口、源或目的IP、源或目的端口）；</p>	1	12
19	云外数据中心托管安全防护服务	<p>1.服务期内以入侵防御系统为支撑工具/设备，基于入侵防御事件库匹配的方式为流经云外数据中心的网络流量提供应用层威胁检测与防护服务。支撑工具/设备符合国产化要求，应配备冗余电源，至少配置1个HA口，1个RJ-45 Console口，1个千兆带外管理口，千兆电口≥ 4个，千兆光口≥ 4个，万兆SFP+接口≥ 8个，可扩展插槽数≥ 5个，2个USB口，并根据实际业务组网需要配备接口光模块及跳线；整机吞吐$\geq 100Gbps$，最大并发连接数$\geq 2000W$，每秒新建HTTP连接数$\geq 50W$。</p> <p>2.系统应支持网线模式部署和透明多口桥部署；</p> <p>3.系统应内置专业的入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、文件上传、代码执行、命令执行、入侵防御特征数量至少在14000条以上；</p> <p>4.支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存。</p> <p>5.支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式。</p>	2	12

			20	Web应用防火墙服务	<p>1.服务期内以Web应用防火墙为支撑工具/设备，为云外数据中心Web应用系统提供HTTP 协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼攻击、SQL 注入、XSS 等攻击防护服务。支撑工具/设备符合国产化要求，应配备冗余电源，至少配置1个HA口，1个RJ-45 Console口，1个千兆带外管理口，千兆电口≥4个，千兆光口≥4个，万兆SFP+接口≥8个,可扩展插槽≥1个，2个USB口，并根据实际业务组网需要配备接口光模块及跳线；整机吞吐≥30Gbps，最大并发HTTP连接数≥1000万，每秒新建HTTP连接数≥15万。</p> <p>2.支持透明模式、代理模式同时部署方式。</p> <p>3.应支持Web应用识别，支持感知服务器的域名、操作系统、Web服务器类型、编程语言、中间件、服务器IP及端口等；</p> <p>4.应具备Web恶意扫描防护的检测与防御能力，专利级别防护能力，基于一种Web服务器恶意攻击的阻断方法、装置及防火墙</p> <p>5.支持协议识别及解码能力，应支持:URL解码、XML解码、JSON解析、Base64解码、Unicode解码、十六进制转换、斜杠反转义、CHR解码、UTF-7解码，支持解析7层以上混合编解码能力，可实现对多层编码攻击的检测；</p>	2	12
			21	态势感知探针服务	<p>1.服务期内以态势感知探针为支撑工具/设备对流经云外数据中心的网络流量进行实时检测，及时发现网络中存在的已知威胁和未知威胁流量，并给态势感知平台提供网络安全数据源服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥4个，千兆光口≥4个，万兆SFP+接口≥4个，RJ-45管理接口≥1个，USB 接口≥4个，内存≥128G，硬盘存储空间≥18T，并根据实际业务组网需要配备接口光模块及跳线；网络流量处理能力≥15Gbps，每秒新建连接数≥10万，最大并发连接数≥800万，应用层性能≥20Gbps。</p> <p>2.支持双向检测事件库≥20000个；</p> <p>3.支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书，对加密流量进行解密及还原；支持SSL3.0，TLS1.0/1.1/1.2；</p> <p>4.持基于工具特征的WEBSHELL检测:如冰蝎连接；</p> <p>5.支持对检测的告警事件结合双向检测机制、原始数据包和关联分析研判模型进行深层次研判给出告警攻击的结果同时根据攻击事件分类给出失陷主机标识，告警结果呈现结果至少包多个维度：告警数据展示、基础数据展示、事件描述、云查情报、流量还原；</p> <p>6.支持通过syslog/kafka/SNMP trap方式将告警日志、违规互联日志、威胁情报日志、流数据日志、协议元数据外发至第三方数据采集平台，支持同时配置多个外发采集平台；</p>	1	12
				云外数据中心			

2	2	安 全 防 护 服 务	1.服务期内以防火墙为支撑工具/设备为云外数据中心提供入侵防御、防病毒、URL控制和流量控制以及基于七元组（源IP、目的IP、入接口（安全域）、服务类型（协议、端口）、APP类型）的安全访问控制策略服务。支撑工具/设备符合国产化要求，应配备冗余电源；千兆电口≥7个，千兆光口≥4个,万兆SFP+接口≥8个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间≥256G，机械硬盘存储空间≥4T；整机吞吐≥80Gbps，TCP新建连接数≥800万/秒。	2	1 2
			2.支持透明、路由、混合、旁路等部署模式。 3.支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护。 4.采用病毒防护引擎；杀毒强度可控，支持快速扫描、全面扫描模式。 5.病毒库不少于140万种病毒特征。 6.内置IPS特征库，特征规则数量不少于9000条，特征库可按分组进行管理。 7.支持HTTP类攻击重定向功能，能够把HTTP协议的攻击类型重定向到指定蜜罐系统，便于对攻击进行审计与分析。 8.支持3个Syslog服务器，发送流量、系统或默认3类型日志到不同服务器； 9.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。		

		23	威胁感知服务	<p>1.服务期内以威胁情报驱动、实战化的网络流量威胁检测与响应平台为支撑工具/设备，为整体网络安全运维服务提供威胁情报支撑。包含以资产暴露，登录入口、文件传输、数据泄漏等视角的全面攻击面梳理能力，覆盖全攻击链路的精准检测与攻击结果判定能力，面向实战的智能聚合分析调查回溯能力，和终端取证、网络阻断的处置闭环能力。基于情报驱动的全流量精准检测、快速响应的解决方案。通过利用云、流量、EDR日志作为输入源，使用威胁情报、规则引擎、建立模型、数据分析获取的多个运算结果关联产出报警，保证报警的高精度，达到减少安全成本，聚焦真实威胁的效果。同时能够区分针对性攻击，对有目的性的攻击突出展示。对于所有攻击数据、可疑行为、以及完整的攻击过程提供完整的存储和查询操作。并实现对黑客入侵过程的完整回溯，对攻击影响面的自动研判，以及对资损情况的自动化收集。以高质量威胁情报为核心，以机器学习、规则、本地防病毒引擎为辅助手段，检测办公网出口流量，精准定位失陷主机，还原威胁传播过程。提供丰富的威胁上下文，终端进程联动定位能力，给安全运维人员处置、溯源提供丰富和准确的参考信息。</p> <p>2.支持代理网环境下的互联网情报源接入和情报查询。</p> <p>3.支持以web查询或API接口查询的方式，查询IOC情报，类型包括IP情报、域名情报、URL情报、文件HASH情报等。</p> <p>4.支持以web查询或API接口查询的方式，查询漏洞情报；</p> <p>5.支持展示多源情报查询结果和历史情报查询信息；</p> <p>6.支持情报大屏展示，内容包括威胁情报地域分布地图、最新威胁情报、情报来源统计、情报类型统计、情报更新量等；</p> <p>7.支持接入安全告警事件，并基于情报生产策略和独有的数据分析模型和情报生产算法进行数据的分析、处理和提取，输出客户独有的高质量IOC情报。</p>	1	12
				核心交换区（流量镜		

2 6	防火 墙 服 务	<p>1.服务期内以防火墙为支撑工具/设备，基于五元组（源IP、目的IP、服务类型（协议、端口））的安全访问控制策略为政务专网广域网边界提供安全访问控制服务。支撑工具/设备符合国产化要求并具备国保证书和检测报告，应配备冗余电源；千兆电口≥ 10个，千兆光口≥ 12个，万兆SFP+接口≥ 4个；可扩展槽位数≥ 2个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间$\geq 128G$；支持IPSec VPN和SSL VPN；整机吞吐$\geq 40Gbps$，最大并发连接数≥ 2000万，每秒新建连接数≥ 26万。</p> <p>2.支持网线模式、透明桥、静态路由、OSPF、策略路由、NAT和端口聚合部署；</p> <p>3.支持三操作系统，可在Web界面完成系统备份、系统恢复、指定启动系统操作；</p> <p>4.支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制；</p> <p>5.为降低支撑工具/设备割接对现有业务的影响，提供现有防火墙策略批量迁移导入方案。</p>	2	1 2
2 7	网 广 域 网 接 入 侵 安 防 系 统 服 务	<p>1.服务期内以入侵防御系统为支撑工具/设备，基于入侵防御事件库匹配的方式为流经政务专网广域网区的网络流量提供应用层威胁检测与防护服务。支撑工具/设备符合国产化要求并具备国保证书和检测报告，应配备冗余电源；千兆电口≥ 10个，千兆光口≥ 4个，万兆SFP+接口≥ 4个；可扩展槽位数≥ 2个，并根据实际业务组网需要配备接口光模块及跳线；硬盘存储空间$\geq 2T$；整机吞吐$\geq 40Gbps$，最大并发连接数≥ 400万，每秒新建连接数≥ 10万。</p> <p>2.系统应支持网线模式、透明桥、静态路由、OSPF、策略路由、NAT和端口聚合；</p> <p>3.支持弱口令检测功能，需支持至少8种网络协议并支持至少7种弱口令检测元素，并文字说明支持的网络协议和定义弱口令的检测元素；</p> <p>4.支持自定义事件升级内容。针对新增加的事件特征，针对不同级别的事件，用户可以选择是否自动升级到自定义策略中。升级界面中至少包含高中低三种级别事件的升级启用选项；</p> <p>5.针对SQL注入和XSS攻击，设备应提供在线事件分析功能，至少提供攻击方法、攻击字段和攻击域、影响的数据库等。</p>	2	1 2

			政务专网数据中	28	入侵防御系统服务	<p>1.服务期内以入侵防御系统为支撑工具/设备，基于入侵防御事件库匹配的方式为流经政务专网数据中心的网络流量提供应用层威胁检测与防护服务。支撑工具/设备符合国产化要求并具备国保证书和检测报告，应配备冗余电源；千兆电口≥10个，千兆光口≥4个，万兆SFP+接口≥4个；可扩展槽位数≥2个，并根据实际业务组网需要配备接口光模块及跳线；硬盘存储空间≥2T；整机吞吐≥40Gbps，最大并发连接数≥400万，每秒新建连接数≥10万。</p> <p>2.系统应支持网线模式、透明桥、静态路由、OSPF、策略路由、NAT和端口聚合；</p> <p>3.支持弱口令检测功能，需支持至少8种网络协议并支持至少7种弱口令检测元素，并文字说明支持的网络协议和定义弱口令的检测元素；</p> <p>4.支持自定义事件升级内容。针对新增加的事件特征，针对不同级别的事件，用户可以选择是否自动升级到自定义策略中。升级界面中至少包含高中低三种级别事件的升级启用选项；</p> <p>5.针对SQL注入和XSS攻击，设备应提供在线事件分析功能，至少提供攻击方法、攻击字段和攻击域、影响的数据库等。</p>	2	12
				29	防火墙服务	<p>1.服务期内以防火墙为支撑工具/设备，基于五元组（源IP、目的IP、服务类型（协议、端口））的安全访问控制策略为政务专网数据中心边界提供安全访问控制服务。支撑工具/设备符合国产化要求并具备国保证书和检测报告，应配备冗余电源；千兆电口≥10个，千兆光口≥4个，万兆SFP+接口≥4个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间≥128G；支持IPSec VPN和SSL VPN。</p> <p>2.支持网线模式、透明桥、静态路由、OSPF、策略路由、NAT和端口聚合部署；</p> <p>3.支持三操作系统，可在Web界面完成系统备份、系统恢复、指定启动系统操作；</p> <p>4.支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制；</p>	2	12

				<p>心 安 全 防 护 服 务</p>	<p>日 志 审 计 服 务</p>	<p>3 0</p>	<p>1.服务期内以日志审计系统为支撑工具/设备，实时不间断地采集政务专网中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，实现全生命周期的日志管理。支撑工具/设备符合国产化要求并具备国保证书和检测报告，应配备冗余电源；千兆电口≥6个，千兆光口≥4个，万兆SFP+接口≥2个，2个USB接口，并根据实际业务组网需要配备接口光模块及跳线；内存≥16G，存储容量≥4TB。</p> <p>2.支持SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC等多种方式完成日志收集功能；</p> <p>3.支持定制任务进行日志数据采集扩展，包括文本格式、目录下文本和数据库格式日志采集，支持编辑正则表达式和SQL语句进行日志采集，支持设置自定义任务时间；</p> <p>4.▲支持全智能范式化解析模式，通过配置原始日志标识库，系统自动识别原始日志，并匹配映射系统通用标准字段，支持解析字段的编辑和调整，确保日志解析的高精度；</p> <p>5.支持系统内置不同审计分析规则，包括各种实时分类监测、历史统计、实时统计等；并支持自定义统计分析</p>	<p>1</p>	<p>1 2</p>
				<p>3 1</p>	<p>数 据 镜 像 交 换 机 服 务</p>	<p>1</p>	<p>1.服务期内以数据镜像交换机为支撑工具/设备，对原始输入流量和预处理后流量按1路信号复制到 N 路信号的线速复制，解决政务外网核心交换机多端口监听旁路设备的需求。</p> <p>2.支撑工具/设备为标准1U机箱，支持24个万兆SFP+插槽（兼容千兆），并根据实际业务组网需要配备接口光模块及跳线；整机吞吐性能≥240Gbps，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。支持4Gbps的高级功能处理能力（切片、去重、时间戳）。</p>	<p>1</p>	<p>1 2</p>

3 2	数据交互安全系统防护服务	<p>1.服务期内以安全隔离与信息交换系统为支撑工具/设备，通过隔离交换矩阵完成应用层数据摆渡，即阻断 OSI模型的七层全部协议为政务外网和政务专网提供网络安全强隔离服务，防止政务外网和政务专网通过网络协议连接。支撑工具/设备符合国产化要求，应配备冗余电源；配备2块液晶屏。内网接口：至少配置1个HA口，1个管理口，千兆电口≥6个，千兆光口≥4个，可扩展槽位数≥2个。 外网接口：至少配置1个HA口，1个管理口，千兆电口≥6个，千兆光口≥4个，可扩展槽位数≥2个， 含全功能模块。并根据实际业务组网需要配备接口光模块及跳线；整机吞吐≥800Mbps，并发连接数≥40万，延时≤1ms。</p> <p>2.设备提供HA工作状态监控灯，可通过HA灯可查看设备HA工作状态，方便设备维护。</p> <p>3.内、外网主机分别具备三系统，即系统A、系统B和备份系统。支持在WEB界面上配置启动顺序，在A系统发生故障时，可以切换到B系统；支持将当前运行系统备份；</p> <p>4.支持文件交换、数据库同步、定制访问、安全传输等数据同步交换功能。</p>	1	1 2
	3 3 防火墙服务	<p>1.服务期内以防火墙为支撑工具/设备，基于五元组（源IP、目的IP、服务类型（协议、端口））的安全访问控制策略为政务外网安全管理区边界提供安全访问控制服务。支撑工具/设备符合国产化要求，应配备冗余电源；千兆电口≥10个，千兆光口≥4个，万兆SFP+接口≥4个；可扩展槽位数≥2个，并根据实际业务组网需要配备接口光模块及跳线；SSD硬盘存储空间≥128G；整机吞吐≥40Gbps，最大并发连接数≥2000万，每秒新建连接数≥26万。</p> <p>2.支持网线模式、透明桥、静态路由、OSPF、策略路由、NAT和端口聚合部署；</p> <p>3.支持三操作系统，可在Web界面完成系统备份、系统恢复、指定启动系统操作；</p> <p>4.支持基于数据包的安全域、地址、用户及用户组、MAC、端口号、服务、域名等进行安全策略控制；</p>	1	1 2

		3 4	堡垒机服务	<p>1.服务期内以堡垒机为支撑工具/设备，从事前预防、事中监控、事后审计的维度把自然人与运维账号进行绑定，避免因账号权限过大、多人使用同一运维账号等造成配置错误、违规操作、运维数据丢失等。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥8个，千兆光口≥4个，1个Console管理口，并根据实际业务组网需要配备接口光模块及跳线；硬盘存储空间≥8TB，带液晶面板，提供不少于500个运维资源授权，内置应用发布软件。</p> <p>2.▲堡垒机和内置应用发布均支持物理旁路，逻辑串联模式，无需镜像、无需改造现有网络结构；</p> <p>3.支持系统管理员、审计管理员、安全管理员三种角色，系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围。</p> <p>4.支持基于角色进行授权访问控制RBAC（Role-Based Access Control），包括系统管理员根据不同角色进行管理工作、运维人员根据不同角色进行运维工作，从而满足最小特权原则、责任分离原则和数据抽象原则；</p> <p>5.支持通过堡垒机授权调用国产化运维工具连接资源进行运维操作；</p> <p>6.支持协议审计和命令管控（SSH/TELNET等）</p> <p>7.支持发布国产化运维工具，实现录像审计（RDP/VNC/X11/HTTP(S)/国产数据库等）</p> <p>8.持用户账号与资源账号的僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常帐号稽核情况报告，方便管理员统计异常账号情况。</p> <p>9.为降低支撑工具/设备割接对现有业务的影响，提供现有堡垒机资产、账号、运维策略批量迁移导入方案。</p>	1 2	1 2

				<p>3 5</p> <p>漏 洞 扫 描 服 务</p>	<p>1.服务期内以漏洞扫描系统为支撑工具/设备，对政务外网中的网络主机、操作系统、数据库系统、网络设备、云计算平台系统漏洞扫描和基线配置核查服务。支撑工具/设备符合国产化要求，千兆电口≥ 6个，1个RJ45 Console口，2个USB接口，并根据实际业务组网需要配备接口光模块及跳线；可扫描IP地址总数无限制，可扫描IP地址数量不限，并发扫描40IP地址。至少包含20种核查类型授权，基线配置核查IP总数量无限制。</p> <p>2.支持扫描的漏洞数量不少于350000个；</p> <p>3.支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、Debian、深度、红旗、麒麟、新支点等；</p> <p>4.支持对主流大数据组件的识别与扫描，包括：Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk、Yarn、Zookeeper，能够扫描的大数据组件漏洞扫描方法不小于300种；</p> <p>5.支持多种协议口令猜测，包括SMB、Snmp、Telnet、SSH、Ftp、RDP、HighGo、MongoDB、kingbase、REDIS等，允许外挂用户提供的用户名字典、密码字典和用户密码组合字典；</p> <p>6.支持扫描容器镜像存在的漏洞，支持扫描互联网上公开仓库中的镜像以及私有仓库中的镜像；</p>	<p>1 2</p>	<p>1 2</p>
				<p>3 6</p> <p>网 站 监 测 服 务</p>	<p>1.服务期内以网站监测为支撑工具/设备，为政务云上各Web门户网站提供网站安全监测，监测内容包括应可用性监测、DNS 域名解析监测、页面变更监测、挂马监测、敏感内容监测等服务。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥ 6个、千兆光口≥ 4个，至少配置1个RJ45 Console口，2个USB接口，并根据实际业务组网需要配备接口光模块及跳线；提供Web漏洞扫描模块、网站监测模块。可扫描和监测子域名或IP总数量≥ 1000个。单个任务的最大并发扫描线程≥ 30个；单域名最大页面数≥ 10000。</p> <p>2.支持对各种Web应用系统的扫描，支持检测SQL注入漏洞、命令注入漏洞、CRLF注入漏洞、LDAP注入漏洞、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等；</p> <p>3.支持Ping、HTTP、GET请求等网站安全监控功能；</p> <p>4.支持基于网站连接通断的可用性监控和基于响应时间的性能监控；</p> <p>5.支持自定义监测周期对网页挂马进行实时监测；</p> <p>6.支持以地图形式展示各类风险统计数据，如漏洞，挂马，篡改，页面变更，域名解析，敏感内容，可自动进行展示数据的切换展示，可展示全网安全状况。</p>	<p>1 2</p>	<p>1 2</p>

			37	日志审计服务	<p>1.服务期内以日志审计系统为支撑工具/设备，实时不间断地采集政务外网中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，实现全生命周期的日志管理。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥6个，千兆光口≥4个，万兆SFP+接口≥2个，2个USB接口，并根据实际业务组网需要配备接口光模块及跳线；内存≥32G，SSD硬盘存储空间≥128G，机械硬盘存储空间≥6TB。可管理设备授权数量≥500个。</p> <p>2.支持SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC等多种方式完成日志收集功能；</p> <p>3.支持定制任务进行日志数据采集扩展，包括文本格式、目录下文本和数据库格式日志采集，支持编辑正则表达式和SQL语句进行日志采集，支持设置自定义任务时间；</p> <p>4.支持全智能范式化解析模式，通过配置原始日志标识库，系统自动识别原始日志，并匹配映射系统通用标准字段，支持解析字段的编辑和调整，确保日志解析的高精度度；</p> <p>5.支持系统内置不同审计分析规则，包括各种实时分类监测、历史统计、实时统计等；并支持自定义统计分析；</p>	1	1 2
				安全集中管控区防护服务	<p>1.服务期内以安全集中管控平台为支撑工具/设备，对全网安全设备的管控，包括特征库升级、策略下发等。支撑工具/设备符合国产化要求，应配备冗余电源，千兆电口≥6个，千兆光口≥4个，内存≥64G，万兆SFP+光口≥2个，并根据实际业务组网需要配备接口光模块及跳线；硬盘存储空间≥48T。支持的集中管理和日志采集设备数量≥100，日志采集性能≥5万条/秒。</p> <p>2.支持全网资产安全状态自动对全网风险等级进行评级，可手动编辑评分规则。</p> <p>3.支持查看全网风险等级、已处置事件数、未处置事件数、处置占比、纳管设备在线数量、纳管设备离线数量、攻击者境外占比、安全事件趋势、资产健康分布、告警日志趋势、威胁类型分级统计。</p> <p>4.支持不少于8块大屏和大屏轮播，支持大屏展示安全态势、关联分析态势、恶意外联态势、横向攻击态势、外部攻击态势、资产态势。</p> <p>5.支持告警研判功能，研判维度包括基本详情、网络负载、告警pcap、全流取证、威胁情报。基本详情可查看基础信息、五元组信息、流信息、告警描述信息；威胁情报维度支持查看威胁类型、地理位置、关联告警。</p> <p>6.支持设备的状态集中监控，包括设备在线离线状态、设备名称、设备类型、设备IP地址、CPU使用率、内存使用率、磁盘使用率、版本信息、流量信息等；</p> <p>7.平台可集中下发检测策略，如包括统一事件策略管理、自定义事件统一下发、白名单统一下发等；</p>	1	1 2

				39	态势感知服务	<p>1.服务期内以态势感知平台为支撑工具/设备，以资产为中心统一采集政务外网中IT资产告警、安全事件信息，提供安全事件分析、调查取证、攻击检测、态势呈现、威胁预警等服务。支撑工具/设备应配备冗余电源、双颗物理CPU 20核，内存≥256G，存储空间≥48TB；数据入库均值≥28000EPS；授权点数≥500点。</p> <p>2.支持不少于10块大屏从多角度多维度的进行态势数据的呈现，包括态势总览、外部攻击态势、资产态势、运行态势、脆弱性态势、风险态势、情报态势、流态势、网站态势、用户行为态势等态势大屏；</p> <p>3.支持对IT资产分组、分域的统一维护能力，具备对全部资产的收集管理能力，包括IP资产、网站资产、组件资产、业务系统以及端口列表，支持资产的增删改查、导入导出、批量处理，多样化展示、多维度关联能力；</p> <p>4.支持对脆弱性统计信息进行集中管理，以图标、圆环图、列表等可视化方式，统一对系统漏洞、弱口令、配置核查、WEB漏洞、渗透漏洞、代码审计漏洞等指标进行统计及处置率呈现。</p> <p>5.支持交互式事件分析模式，提供不少于360条内置的策略，并支持自定义策略、收藏的策略等类型，点击策略名称可进行快速应用，收藏的策略可设置为默认策略使用，支持策略的导入导出。</p> <p>6.支持攻击技战术的预测能力，支持根据前序安全事件时间、前序攻击技术、攻击场景通过预测模型，预测下一小时和第二天发生的攻击技术和发生概率，并在ATT&CK模型展示预测页面突出展示；</p> <p>7.系统支持不少于多个主流厂家设备对接，包括但不限于深信服、绿盟、微步在线、华为、H3C、山石网科、知道创宇、迪普科技、安博通、天融信、启明星辰、网御星云等。</p> <p>8.内置多个联动动作，包括但不限于向群发送消息、发送飞书、发送短信、新建安全策略、策略下发、获取下发任务列表、新增黑名单、删除黑名单、IP解封、执行脚本等；</p> <p>9.支持与防火墙、漏洞扫描、态势感知探针、网站检测等设备的联动防护，提供日志的采集和数据的接口对接，通过SOAR剧本实现策略的自动化响应</p>	1	12
				40	数据镜像交换机服务	<p>1.服务期内以数据镜像交换机为支撑工具/设备对原始输入流量和预处理后流量按1路信号复制到 N 路信号的线速复制，解决政务外网核心交换机多端口监听旁路设备的需求。</p> <p>2.支撑工具/设备为标准1U机箱，支持24个万兆SFP+插槽（兼容千兆），并根据实际业务组网需要配备接口光模块及跳线；整机吞吐性能≥240Gbps，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。</p> <p>3.支持4Gbps的高级功能处理能力（切片、去重、时间戳）。</p>	1	12

			4 1	远程安全接入服务	<p>1.服务期内以符合国密算法的安全接入网关为支撑工具/设备，提供持多种身份认证方式、细粒度访问权限控制等服务，保证远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全，符合国家商用密码标准和国产化要求，具有快速、易用、全面等优势。授权用户数≥ 4000个。</p> <p>2.客户端支持龙芯、兆芯、飞腾、鲲鹏等国产化CPU平台，支持中标麒麟，银河麒麟、普华、深度OS、优麒麟、UOS统信、中科方德等国产化操作系统客户端；</p> <p>3.支持自定义虚拟门户，可在一台设备上为不同用户群配置多种登录门户，支持域名或者IP地址访问。</p> <p>4.产品支持多系统引导，即系统A、系统B和备份系统，可在管理员界面直接配置启动顺序，支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且配置文件分别支持加密导入导出。</p> <p>5.持WebVPN跨平台免插件访问，基于泛域名或多端口方式发布Web资源，支持Windows、Mac、Linux、国产化UOS\银河麒麟V10等系统主流浏览器，如Chrome、Firefox等最新版，免插件免客户端使用VPN接入内网。</p>	1	1 2
			4 2	资产与脆弱性管理服务	<p>1.服务期内以资产与脆弱性管理系统为支撑工具/设备，通过资产探测和描绘、资产属性维护、资产合规分析、脆弱性管理、漏洞优先级处置评估、漏洞影响评估、漏洞跟踪处置、工单流转、报告报表、情报预警等进行资产和脆弱性问题多维分析，以多源兼容、关联补全、智能调度、协同分析、精准投放为特色，从资产问题发现、问题确认处置进行闭环管理，解决资产和脆弱性梳理、资产安全问题分析、脆弱性消解和缓减的闭环处理。产品软硬一体形态，通过资产指纹和属性数据、漏洞采集和关联分析、情报碰撞辅助分析等进行资产风险数据分析，同时运用脆弱性预评估模型，梳理出资产典型安全问题；从摸清家底管理家底的角度主动对抗被攻击的风险，内置资产漏洞发现分析，资产漏洞跟踪、资产脆弱性闭环流转管理、报告报表等功能实现资产风险问题持续跟踪和优化。</p> <p>2.具备资产管理能力，支持资产台账管理，且支持资产数据导入导出批量操作，支持资产业务标签和位置标签标记管理，资产属性展示配置列可自定义</p> <p>3.支持对漏扫引擎、核查引擎、弱口令引擎以及web漏扫引擎进行分类集中管理，并下发扫描任务，收集扫描结果进行集中管理跟踪；</p> <p>4.支持多维度漏洞信息查询或筛选，包括但不限于资产名称、漏洞名称、IP/URL、发现时间、处置时间、处置人员、漏洞等级、漏洞来源、漏洞状态；</p> <p>5.支持通过脆弱性跟踪任务查看漏洞跟踪状态、待处理的漏洞、整改中的漏洞、已修复漏洞、归档漏洞等。支持管理各任务内漏洞修复状态包括处置节点、误报、无法整改、处置归档等进行记录跟踪；</p>	1	1 2

		蜜罐服务	<p>1.服务期内以蜜罐为支撑工具/设备，模拟真实的系统和服务，如服务器、数据库等，吸引攻击者的注意力，将他们从真正有价值的目标上引开。增加攻击者在蜜罐上花费时间和精力，减少对真实业务系统的威胁，为防护措施争取更多时间，提升主动防御能力。支撑工具/设备，符合国产化要求，应配备冗余电源，配置≥6个千兆电口、≥4个千兆光口、4个万兆光口、≥1个接口扩展槽位，并根据实际业务组网需要配备接口光模块及跳线；硬盘存储空间≥4T；支持系统服务仿真、数据库仿真、应用仿真等不少于20个，应提供攻击行为捕获、攻击数据分析和告警上报等功能。</p> <p>2.具备蜜网组网功能，进行蜜网的多网段组网，支持设置蜜网部署网段，保证蜜网的高度仿真。</p> <p>3.支持蜜网配置，包括绑定服务、安全策略、编辑蜜网、删除蜜网操作；模拟的蜜罐可配置为允许与外部网络进行通信，以模拟更真实的网络交互；</p> <p>4.支持智能化蜜网部署，自动化扫描指定网段，智能化部署网段，同时可根据指定网段真实服务的变化自动调整蜜罐服务；</p> <p>5.支持数据库类蜜罐，包括但不限于：Mysql、Mysql溯源、PostgreSQL、redis；</p> <p>6.支持Windows主机诱饵，包括但不限于：浏览器书签、主机hosts文件、浏览器搜索历史、Cookies、Ftps、Xshell、Windows凭据、RDP远程登录；</p>	1	1 2

			<p>服务期内以安全管理制度知识库子模块为支撑工具/设备，提供统一安全运营服务过程中产生的各类安全管理制度文档、知识文档等，功能包括知识库归类设置、知识文档上传、知识文档审核、知识库综合查询等功能。</p> <p>具体服务目标、范围和内容：</p> <p>1.服务目标：统一安全运维服务过程中产生的各类安全管理制度文档、知识文档等，安全管理制度知识库子模块为各类文档提供统一存储管理服务。</p> <p>2.服务范围：覆盖西安市政务外网，市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点），统一安全运维服务过程中产生的各类安全管理制度文档、知识文档提供统一存储管理的系统。</p> <p>3.服务内容：安全管理制度知识库子模块功能包括：知识库归类设置、知识文档上传、知识文档审核、知识库综合查询等功能。</p> <p>（1）知识库归类设置</p> <p>需设置哪些知识库文档为必须上传，与项目信息进行管理。</p> <p>（2）知识文档上传</p> <p>格式支持pdf、doc、xls等，同时支持视频文件上传。</p> <p>（3）知识文档审核</p> <p>对上传的文档进行审核，审核不通过的，要有审核不通过的原因。</p> <p>（4）知识库综合查询</p> <p>按照不同阶段、不同项目对知识库文档进行检索、浏览。支持按照文件标题、文件内容、标题等信息对知识库进行查找，同时知识库提供情报在线查询，可在线查询ip、域名、url的定位、威胁等级等信息。</p> <p>（5）文档管理功能</p> <p>提供文档类型、信息类型等知识文件的管理功能，支持文档类知识管理，可上传下载文档形成文档类资料，支持自定义知识分组、知识条目批量导入导出、事件处置流程信息归档等。</p>	
--	--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		45	人 管 理 服 务	<p>服务期内以人员管理子模块为支撑工具/设备，提供统一管理和维护主管单位人员、各类厂家人员信息维护、账号认证服务及授权等服务。具体服务目标、范围和内容：</p> <p>1.服务目标：统一维护主管单位人员和各类厂家人员的信息维护、账号认证服务及授权服务等。</p> <p>2.服务范围：覆盖市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点），安全管理、安全服务、安全设备维护等涉及一体化安全运维人员的信息维护、账号认证服务及授权服务等。</p> <p>3.服务内容</p> <p>（1）人员信息管理：人员添加删除，确保人员与实际情况相符。维护人员的基本信息，包括姓名、性别、年龄、联系方式、职责、保密协议、调岗离职事务交接清单等。</p> <p>存储人员的详细履历，如教育背景、工作经历、专业资质证书、无犯罪记录等，方便随时查阅和更新。支持上传人员照片，增强信息的直观性和完整性。</p> <p>（2）权限管理:根据人员的职责，精确分配其在系统和相关工具中的操作权限。例如，安全管理员具有系统配置权限，而普通安全监测人员只有数据查看和基本分析权限。实现权限的动态调整，当人员岗位变动或临时承担特定任务时，能快速更新其权限，确保访问控制的严格性和灵活性。记录权限变更历史，以便追溯和审计，防止权限滥用和安全漏洞。</p>	
				<p>业务系统全生命周期安全管理服务</p> <p>服务期内以业务系统全生命周期安全管理子模块为支撑工具/设备，提供高效、完善的业务系统全生命周期安全管理系统，包括等级保护备案测评信息、密评备案和测评信息等，以提升信息安全管理水平，满足监管要求，并为各相关部门提供有力支持。具体服务目标、范围和内容：</p> <p>1.服务目标：随着政务信息化推动政府治理能力现代化，各委办局的上云需求日益增长，为确保政务云环境下业务系统的安全性和合规性，需一套高效、完善的业务系统全生命周期安全管理系统，以提升信息安全管理水平，满足监管要求，并为各相关部门提供有力支持。</p> <p>2.服务范围：覆盖市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点），各委办局所部署使用的各类业务系统。</p> <p>3.服务内容</p> <p>（1）等保合规管理：记录业务系统的等保定级信息，包括系统等级、测评时间、测评机构、测评结果等，并及时更新相关数据，确保对每个业务系统的等保状态清晰明了。</p> <p>（2）密评合规管理：密评信息：详细记录商用密码应用情况，密评的结果，便于跟踪密评整改情况，保证业务系统密码应用的安全性和合规性。</p>	
				<p>服务期内以协同处置子模块为支撑工具/设备，提供整合各方资源和能力，实现网络安全事件快速、高效协同处置。包括信息共享与沟通协作、事件监测与预警、应急指挥与调度、动态应急处置、资源管理与协调、重大保障等。具体服务目标、范围和内容如下：</p> <p>1.服务目标：整合各方资源和能力，实现网络安全事件快速、高效协同处</p>	

[illegible]

					<p>能指标数据、告警数据、拓扑数据等的管理功能。实时掌握市政务外网网络安全基础设施运行状态，同时为安全运维管理人员提供工具支撑。具体服务目标、范围、内容如下：</p> <p>1.服务目标：安全运维管理子模块对市政务外网网络基础设施的安全资源进行统一管理、监控纳管，完成资源数据、监控性能指标数据、告警数据、拓扑数据等的管理功能。实时掌握市政务外网网络安全基础设施运行状态，同时为安全运维管理人员提供工具支撑。</p> <p>2.服务范围：覆盖西安市政务外网、市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点），所涉及各类安全平台、安全设备、安全运维人员。</p> <p>3.服务内容</p> <p>（1）网络安全拓扑图：实现拓扑图的动态绘制与管理。</p> <p>（2）监控探针：针对政务云的网络设备、安全设备、主机设备、存储设备、终端设备、中间件、应用系统等目标对象，能够提供相应的探针实现系统的性能指标、日志、调用链等信息的采集。</p> <p>（3）运维数据自动发现：通过网络协议等方式采集主机、网络、安全等硬件设备的信息。</p> <p>（4）运维数据采集治理：对于设备台账、机房设备、端口策略、漏扫结果、防病毒日志等非实时数据，使用主动汇总，由平台主动调用第三方产品接口或直连数据库的方式汇总数据。对于网络流量、入侵监测告警、入侵防御告警、安全防护软件运行日志、设备操作日志等实时类数据，使用被动接收的方式，在第三方产品配置平台为日志接收方，将日志转发至平台。</p> <p>（5）资产监控管理：实现软硬件资源的集中化、规范化、标准化管理。提供IT资源对象的全生命周期管理功能的同时为运维管理平台提供数据支撑,实现资源盘点、容量管理等数据场景。</p> <p>（6）基础设施监控：实现针对专用计算机软硬件环境（包含物理机、云平台等）以及基础应用提供运行监控、性能探测、阈值告警以及对服务端软件提供安装部署、卸载，以及版本控制等配置管理等功能。</p> <p>（7）应用可用性探测：对业务系统进行分级分类，按照不同级别实现对业务应用及系统组件运行状态的连续探测，7*24小时模拟用户请求，从真实的用户体验角度判断业务系统的可用性，帮助提前预警故障并快速定位，保证服务的连续性。</p> <p>（8）告警中心：实现告警服务集成、告警处理、通知策略管理，提供告警级别定义、告警级别提升管理。需提供告警集中、告警压缩、告警恢复、告警关闭。</p> <p>（9）运维服务：实现基于工单、监控、知识、通知以及轮值排班等功能实现搭建运维人员操作入口。</p> <p>（10）运维流程服务：实现基于工单的信息，指定其中一个信息统计对工单进行统计。</p> <p>（11）报告中心：实现对各委办局相关业务系统整体网络的运维监控及</p>		
--	--	--	--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

49	安 全 服 务 管 理	保密监管态势通过报告形式进行呈现展示。
		<p>服务期内以安全服务管理子模块为支撑工具/产品，提供对项目全流程、全过程的管理；项目协同办公管理，解决多厂家沟通，提高效率、减少、杜绝了互相推诿；多项目、大项目的进度情况、人力投入实时掌握；项目每阶段人员投入，和合同原定保持同步一致，防止厂家“重合同签订、轻项目建设”情况；涵盖项目管理全过程全监管；项目审计清晰跟踪、项目验收（初验和竣工）完成“线上办公、线上查阅、竣工验收”，实现验收电子化；实现所有项目建设情况的总览、项目总进度实时掌握。具体服务目标、范围、内容如下：</p> <p>1.服务目标：满足安全服务管理子模块对项目全流程、全过程管理；项目协同办公管理，解决多厂家沟通，提高效率、减少、杜绝了互相推诿；多项目、大项目的进度情况、人力投入实时掌握；项目每阶段人员投入，和合同原定保持同步一致，防止厂家“重合同签订、轻项目建设”情况；涵盖项目管理全过程全监管；建立知识库沉淀、共享共用管理，沉淀项目建设全周期的过程文档，形成知识库；项目审计清晰跟踪、项目验收（初验和竣工）完成“线上办公、线上查阅、竣工验收”，实现验收电子化；实现所有项目建设情况的总览、项目总进度实时掌握。</p> <p>2.服务范围：覆盖西安市政务外网、市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点），所涉及各类安全平台、安全设备、安全运维人员。</p> <p>3.服务内容</p> <p>提供项目文档管理、合同管理、会议管理、考核管理、竣工管理等功能。</p>

2.安全运维服务要求

序号	服务内容	服务人数	服务时间（月）	备注
1	<p>1.服务期内至少提供2名高级安全运维人员、3名中级安全运维人员和5名初级安全运维人员。</p> <p>2.以上安全运维人员提供驻场安全运维服务，包括日常运维服务、应急响应及处置服务、重大活动保障服务、安全监测服务、安全通告服务。</p>	10	12	<p>2名高级</p> <p>3名中级</p> <p>5名初级</p>

3.安全管理体系服务要求

序号	服务内容	安全服务体系说明
1	安全管理体系	提供安全管理体系服务包含安全保障顶层设计服务、安全管理制度修订服务、安全防护标准评估服务、租户上云安全标准制定服务、安全操作规范考核标准服务、安全运维流程监督标准制定服务

2	安全风险评估	提供安全风险评估服务，为2025年迁移上云的业务系统及政务云存量业务系统，按照市政务云平台安全管理相关要求，依据《GBT 20984-2022 信息安全技术 信息安全风险评估方法》中对风险评估的相关要求需要进行安全风险评估，业务系统风险评估不少于120个。
3	安全培训服务	次数：不少于4次；时间：每次不少于4小时。
4	安全咨询服务	专项服务：重保、专项咨询服务均不少于4次、设计1次。

4.交付要求

4.1.基础安全防护服务交付物要求

序号	一级服务名称	二级服务名称	数量	备注
1	政务外网广域网接入安全防护服务	防火墙	2	自带设备
2		态势感知探针	1	
3	互联网行政办公区安全防护服务	负载均衡	2	
4		上网行为管理设备	2	
5		防火墙	2	
6	互联网业务发布区安全防护服务	负载均衡	2	
7		运营商级抗DDoS	2	
8		抗DDoS	2	
9		防火墙	2	
10	局域网区（市政府、市委、综合楼）安全	防火墙	6	
11		态势感知探针	1	
12	政务云平台（凤八）安全防护服务	防火墙	2	
13	政务云平台（西咸）政务外网区安全防	防火墙	2	
14	护服务	交换机	2	
15		防火墙	2	
16		抗DDoS	2	
17		威胁感知	1	
18		全流量分析	1	
19	云外数据中心托管区安全防护服务	入侵防御系统	2	
20	云外数据中心安全防护服务	Web应用防火墙	2	
21		态势感知探针	1	
22		防火墙	2	
23	核心交换区（流量镜像分析）安全防护	威胁感知	1	
24		全流量分析	1	
25	政务专网局域网区（市政府、市委、综	防火墙	6	
26	合楼）安全防护服务	防火墙	2	
	政务专网广域网接入安全防护服务	防火墙	2	

27		入侵防御系统	2
28	政务专网数据中心安全防护服务	入侵防御系统	2
29		防火墙	2
30		日志审计	1
31		数据镜像交换机	1
32	数据交互区安全防护服务	数据交换系统	1
33	安全监管控制区防护服务	防火墙	1
34		堡垒机	1
35		漏洞扫描平台	1
36		网站监测平台	1
37		日志审计系统	1
38		安全集中管控平台	1
39		态势感知平台	1
40		数据镜像交换机	1
41		远程安全接入	1
42		资产与脆弱性管理	1
43		蜜罐	1
44	一体化安全运维平台服务	安全管理制度知识库 服务	1
45		人员管理服务	1
46		业务系统全生命周期 安全管理服务	1
47		协同处置服务	1
48		安全运维管理服务	1
49		安全服务管理	1

4.2安全运维服务交付成果

序号	服务名称	交付成果
1	日常运维服务	《周报》、《月报》、《季报》、《年报》 《资产台账》 《日常运维服务实施方案》
2	应急响应及处置服务	应急预案 安全事件应急响应报告
3	重大活动保障服务	《重大活动保障方案》 《重大活动保障应急预案》 《重大活动保障监控日报》 《重大活动保障总结报告》 《重保期间应急响应报告》

4	安全监测服务	《周、月、年度安全态势总结》 《安全策略分析与优化》
5	安全通告服务	《安全漏洞通告》 《安全漏洞周报》

4.3 安全管理体系服务交付物要求

序号	服务名称	交付成果
1	安全保障顶层设计服务	《政务信息化公共基础平台安全风险状况评估报告》 《政务信息化公共基础平台安全管理体系手册》
2	安全管理制度修订服务	《基础设施类安全管理制度汇编》 《管理类安全制度汇编》 《工作类安全制度汇编》 《人员安全管理制度》 《物理和环境安全管理制度》 《资产安全管理制度》 《网络安全保密管理制度》
3	安全防护标准评估服务	《网络边界安全防护标准》 《租户上云风险评估标准》 《业务系统分级分类防护标准》
4	云上租户安全标准制定服务	《云上租户安全责任边界》 《云上租户安全考核办法》
5	安全操作规范考核标准服务	《例行操作安全规范》 《安全操作交付管理规范》 《安全操作运维服务目录》 《例行操作安全规范》 《安全操作交付管理规范》
6	安全运维流程监督标准制定服务	《资产使用类流程访问控制开通流程》 《安全事件管理流程》 《工单安全处置流程》 《安全监测操作管理流程》
7	风险评估报告	政务云上120个业务系统风险评估报告，包括但不限于： 《信息系统资产梳理表》 《信息系统渗透测试报告》 《信息系统漏洞扫描报告》 《信息系统风险评估报告》
8	安全培训	《安全培训方案》 《安全培训课件》 《培训总结报告》

采购包2： 标的名称：监理服务		9	安全咨询	《重保咨询方案/报告》*4 《专项咨询方案/报告》*4 《安全咨询设计方案》*1
序号	参数性质	技术参数与性能指标		
		<p>一、监理服务要求（包括但不限于以下内容）</p> <p>（一）监理范围：对项目运维服务期全过程监理，确保运维服务的规范性、质量和效率，对运维过程进行监督、控制和绩效评价。前期提供项目技术咨询；协助审核有关合同、协议；进行项目质量、项目进度等的控制；进行有关技术文档等文件的管理；对项目内容进行全生命周期咨询监理；定期向建设单位汇报项目进展情况，提交项目监理服务报告；代表建设单位协调与承建单位的工作关系和协调解决项目实施过程中的各类纠纷，确保本项目按期、保质、顺利地完成。</p> <p>（二）服务方式：监理公司应委派总监理工程师和现场监理工程师，建立项目监理组并提供现场监理服务，负责整个项目运维的全程监理工作，且每周向甲方提交监理周报并召开协调会或专题会。</p> <p>（三）服务内容：</p> <p>1.项目组织及实施方案监理</p> <p>（1）协助业主对本项目运维过程进行现场监理、提供项目运维方案的咨询和审核意见；</p> <p>（2）审核和确认运维单位的实施人员组织和实施计划安排；</p> <p>（3）审核和确认运维单位的质量保证计划；</p> <p>（4）审核和确认运维单位的进度控制计划。</p> <p>2.工程组织及总体技术方案的质量控制</p> <p>（1）协助审查项目承建单位的投标响应文件、合同及运维方案；审核运维服务方案、流程设计（如ITIL框架下的服务目录、SLA协议）是否符合项目目标和行业标准。</p> <p>（2）在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；</p> <p>（3）检查运维管理制度（如安全规范、应急预案、变更管理流程）的完整性和可操作性。</p> <p>3.工程质量控制</p> <p>（1）审核施工单位的运维方案；</p> <p>（2）对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；</p> <p>（3）对SLA合规性，监控服务级别协议（SLA）执行情况（如系统可用性、故障响应时间），定期生成合规性报告。；</p> <p>（4）绩效评估：通过KPI（如MTTR平均修复时间、用户满意度）评估运维团队表现，提出改进建议，监督审查考核工作，评估培训效果。</p> <p>（5）对监理项目运维过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版；</p> <p>4.安全与风险控制</p> <p>（1）安全检查，监督安全策略执行（如漏洞扫描、日志审计、权限管理），确保符合等保2.0等法规要求；</p> <p>（2）风险预警，识别潜在风险（如数据泄露、单点故障），推动整改措施；</p> <p>5.事件进度控制与问题管理</p> <p>（1）建立进度控制协调制度，落实进度控制责任；</p> <p>（2）故障处理监督，跟踪重大故障的响应、根因分析及解决进度，验证闭环处理效果；</p> <p>（3）预防性建议，根据事件趋势分析，提出优化建议（如容量扩容、流程优化），以确保项目</p>		

的阶段和总体进度目标的实施。

6.投资、变更控制

- (1) 完善职责分工及有关质量项目管理制度，落实投资控制的责任；
- (2) 督促承建单位按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度。
- (3) 变更控制，审核系统变更（如版本升级、架构调整）的合规性，评估影响范围，避免未经授权变更。

- (4) 核查CMDB（配置管理数据库）的准确性，确保资产信息与实际一致。

7.合同管理

- (1) 以合同为依据，本着“实事求是、公正”的原则，处理合同执行过程中的各种争议；
- (2) 分析、跟踪和检查合同执行情况，确保按时履约；
- (3) 对合同的工期的延误和延期进行审核确认；
- (4) 对合同变更、索赔等事宜进行审核确认；
- (5) 根据合同约定，审核项目运维单位的支付申请；
- (6) 建立合同目录、编码和档案。

8.项目信息文档管理

- (1) 文档审核，确保运维文档（如拓扑图、操作手册、巡检记录）完整且及时更新；
- (2) 监督运维团队的知识共享（如案例库、培训记录），避免依赖个人经验；
- (3) 及时向采购人提交反映项目动态和监理工作情况的项目文档；
- (4) 做好双方合同、测试文档、验收报告等各类往来文件的存档；
- (5) 建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况；
- (6) 督促、检查运维单位及时完成各阶段设备资料、工程技术资料的整理和归档工作；
- (7) 转达采购人发出的指示、通知和业务联系单。

9.项目文件的管理

- (1) 监理方应负责以下文档的编写：项目建设监理日志、周报、月报及项目大事记；项目协调会、监理例会等各类会议的纪要；阶段性项目总结、阶段性项目监理总结、各类监理通知；
- (2) 监理方应参与以下文档的管理：项目实施期间各类技术文件、合同执行过程中的各类往来文件及存档。

10.项目组织协调

为保证监理工作的开展和实施协调，监理方组织必要的会议来保证：

- (1) 项目协调会、专题会；组织定期会议（如周报、月度评审），协调业主方与运维团队的需求冲突；
- (2) 提供监理周报/月报，汇总运维状态、问题及改进建议；
- (3) 监督各方履行职责，协调各方的工作关系；
- (4) 建立畅通的沟通平台和沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积极协调项目各方之间的关系，推动项目实施过程中问题的解决；
- (5) 确立项目安全监督的工作目标。

11.项目初验和试运行阶段

- (1) 协助建设单位制定验收程序和标准，审查验收方案和验收文档。
- (2) 对运维服务周期（如年度服务）进行验收，审核交付物是否符合合同要求，确保符合ISO 20000、ITSS等运维服务标准。

		<p>(3) 基于运维数据分析，提出自动化、智能化升级方案（如引入AIOps工具）。</p> <p>(4) 协调与承建单位之间的关系，解决纠纷。</p> <p>(5) 监督、检查并督促承建单位对用户的培训工作。</p> <p>12.项目正式验收阶段</p> <p>(1) 审核竣工文档资料的完整性、可读性及其与项目实际的一致性。</p> <p>(2) 审查承建单位提交的正式验收申请，编写项目质量评估报告。</p> <p>(3) 参加项目正式验收，签署正式验收意见。</p> <p>(4) 审查承建单位提交的竣工结算申请并报建设单位。</p> <p>(5) 编制/整理项目监理资料归档文件并报建设单位审核无误后，移交建设单位存档。</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.2.3人员配置要求

采购包1:

服务期内至少提供2名高级安全运维人员、3名中级安全运维人员和5名初级安全运维人员。以上安全运维人员提供驻场安全运维服务，包括日常运维服务、应急响应及处置服务、重大活动保障服务、安全监测服务、安全通告服务。

采购包2:

本项目配备专业的监理服务团队，至少包括以下人员：总监理工程师1名，总监理工程师代表1名，专业监理工程师至少3名。以上人员具备信息系统监理师资格证书。

3.2.4设施设备配置要求

采购包1:

满足项目需求

采购包2:

满足项目需求

3.2.5其他要求

采购包1:

无

采购包2:

无

3.3商务要求

3.3.1服务期限

采购包1:

合同签订30日之内中标单位应具备服务能力，服务期为监理单位出具服务能力审核报告之日起12个月。

采购包2:

合同签订之日起至项目运维合同服务期结束，投标人按本项目合同规定移交完所有监理文件，服务项目完成终验之日止。

3.3.2服务地点

采购包1:

采购人指定地点

采购包2:

采购人指定地点

3.3.3考核（验收）标准和方法

采购包1:

验收：投标人按照采购文件及合同内容提供完整服务，服务期满且无争议，考核合格，视为验收合格。验收过程中，若

发现严重质量问题，且在规定时间内整改无效，采购人将进行严肃处理，并将其列入“不良行为记录名单”。验收依据 招标文件、投标文件、合同文本、国内相应的标准、规范。

采购包2:

验收：投标人按照采购文件及合同内容提供完整服务，服务期满且无争议，考核合格，视为验收合格。验收过程中，若发现严重质量问题，且在规定时间内整改无效，采购人将进行严肃处理，并将其列入“不良行为记录名单”。验收依据 招标文件、投标文件、合同文本、国内相应的标准、规范。

3.3.4支付方式

采购包1:

分期付款

采购包2:

分期付款

3.3.5.支付约定

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

采购包1：付款条件说明：服务期满6个月，服务商完成本合同约定的全部服务内容的开通，在15个工作日内组织中期验收，验收通过后，达到付款条件起 30 日内，支付合同总金额的 40.00%。

采购包1：付款条件说明：服务期届满后15个工作日内组织终验，验收通过后，达到付款条件起 45 日内，支付合同总金额的 30.00%。

采购包2：付款条件说明：合同签订后，达到付款条件起 10 日内，支付合同总金额的 30.00%。

采购包2：付款条件说明：服务商完成本合同约定的全部服务内容的开通、服务期满6个月后，在15个工作日内组织中期验收，验收通过后，达到付款条件起 30 日内，支付合同总金额的 40.00%。

采购包2：付款条件说明：服务期届满后15个工作日内组织终验，验收通过后，达到付款条件起 45 日内，支付合同总金额的 30.00%。

3.3.6违约责任与解决争议的方法

采购包1:

1.按《民法典》中的相关条款执行。2.未按合同要求提供服务或不能满足服务要求的，采购单位有权终止合同，并对乙方违约行为进行追究，乙方除应按合同总金额20%向甲方支付违约金外，还应赔偿由此引致甲方损失。3.投标人应保证其提供的服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由供应商承担全部责任。任何被供应商用于未经授权的商业目的行为所造成的违约或侵权责任由供应商承担。

采购包2:

1.按《民法典》中的相关条款执行。2.未按合同要求提供服务或不能满足服务要求的，采购单位有权终止合同，并对乙方违约行为进行追究，乙方除应按合同总金额20%向甲方支付违约金外，还应赔偿由此引致甲方损失。3.投标人应保证其提供的服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由供应商承担全部责任。任何被供应商用于未经授权的商业目的行为所造成的违约或侵权责任由供应商承担。

3.5其他要求

本项目为服务类项目采购，其中所涉及的设备均为租赁，服务期为12个月。

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	资格审查要求概况	评审点具体描述	关联格式
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。	资格证明文件 投标函
2	供应商应提供健全的财务会计制度的证明材料；	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。	资格证明文件
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

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	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。	资格证明文件 投标函
2	供应商应提供健全的财务会计制度的证明材料；	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。	资格证明文件
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	资格审查要求概况	评审点具体描述	关联格式
----	----------	---------	------

1	营业执照	具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。	资格证明文件
2	法人代表授权书	法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。	资格证明文件
3	财务状况报告	法人提供经审计的2023年度或2024年度的财务报告或提交投标文件递交截止时间前一年内银行出具的资信证明；其他组织和自然人提供银行出具的资信证明或财务报表；或政府采购信用担保机构出具的《政府采购投标担保函》。	资格证明文件
4	税收缴纳证明	提供投标文件递交截止时间前近一年内至少一个月已缴纳的纳税凭据或完税证明；依法免税的供应商应提供相关文件证明。	资格证明文件
5	社会保障资金缴纳证明	提供投标文件截止时间前近一年内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。	资格证明文件
6	具有履行本合同所必需的设备和专业技术能力	提供具有履行本合同所必需的设备和专业技术能力的承诺书。	资格证明文件
7	政府采购活动前三年内在经营活动中没有重大违法记录	提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。	资格证明文件

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照	具有独立承担民事责任能力的法人、其他组织或自然人，提供营业执照/事业单位法人证书/非企业专业服务机构执业许可证/自然人身份证。	资格证明文件
2	法人代表授权书	法定代表人参加投标时，提供法定代表人证明书；授权代表参加投标时，提供法定代表人授权书；非法人单位参照执行。	资格证明文件
3	财务状况报告	法人提供经审计的2023年度或2024年度的财务报告或提交投标文件递交截止时间前一年内银行出具的资信证明；其他组织和自然人提供银行出具的资信证明或财务报表；或政府采购信用担保机构出具的《政府采购投标担保函》。	资格证明文件

4	税收缴纳证明	提供投标文件递交截止时间前近一年内至少一个月已缴纳的纳税凭据或完税证明；依法免税的供应商应提供相关文件证明。	资格证明文件
5	社会保障资金缴纳证明	提供投标文件截止时间前近一年内已缴存的至少一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明，依法不需要缴纳社会保障资金的单位应提供相关证明材料。	资格证明文件
6	具有履行本合同所必需的设备和专业技术能力	提供具有履行本合同所必需的设备和专业技术能力的承诺书。	资格证明文件
7	政府采购活动前三年内在经营活动中没有重大违法记录	提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明。	资格证明文件

4.3落实政府采购政策资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	本采购包专门面向中小企业采购	参与的供应商（联合体）服务全部由符合政策要求的中小企业承接。监狱企业、残疾人福利性单位视同为中小企业。	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

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》等法律法规，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 and 标准对待所有的投标人。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。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

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。采购人代表可以使用采购人代表专用签章确认评审意见。

三、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

采购包2：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，必须以本招标文件的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	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	1.在评标过程中，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 分项报价表 标的清单

2	报价不得超过公布的购预算或最高限价	报价不得超过公布的采购预算或最高限价，否则投标文件作为无效处理。	开标一览表 分项报价表
3	投标有效期	投标有效期是否满足招标文件要求。	投标函
4	商务响应情况	商务响应情况，若负偏离，投标文件作为无效处理。	商务应答表
5	其他实质性条款	出现不符合法律、法规和招标文件中规定的其他实质性要求的情况，投标文件作为无效处理。	商务应答表 投标文件封面

采购包2:

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	1. 在评标过程中，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 分项报价表 标的清单
2	报价不得超过公布的购预算或最高限价	报价不得超过公布的采购预算或最高限价，否则投标文件作为无效处理。	开标一览表 分项报价表
3	投标有效期	投标有效期是否满足招标文件要求。	投标函
4	商务响应情况	商务响应情况，若负偏离，投标文件作为无效处理。	商务应答表
5	其他实质性条款	出现不符合法律、法规和招标文件中规定的其他实质性要求的情况，投标文件作为无效处理。	商务应答表 投标文件封面

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应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应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

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选供应商、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

- （一）分值汇总计算错误的；
- （二）分项评分超出评分标准范围的；
- （三）评标委员会成员对客观评审因素评分不一致的；
- （四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评审，重新评审改变评标结果的，书面报告本级财政部门。

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。

采购包2：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、评标方法和标准；
- 四、开标记录和评标情况及说明，包括投标无效投标人名单及原因；
- 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、说明或者更正，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

（综合评分法适用）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：

评审因素	评审标准
------	------

分值构成		详细评审 90.00 分 报价得分 10.00 分			
评审因素 分类	评审项	详细描述	分值	客观/主观	关联格式
	项目分析	根据投标人对项目整体及重点难点的分析赋分。 了解项目实施过程中的重点难点，并提出科学合理的应对策略，得 5 分； 提供了相关分析， 但内容简单，无应对策略，得 3 分； 相关分析或与实际不符，得 1 分； 未提供项目分析，得 0 分。	5.0000	主观	服务方案
	标▲技术参数	根据投标人对技术要求中基础安全防护服务标注“▲”的技术响应情况赋分： 完全满足招标文件要求的，得 15 分，每项负偏离扣 3 分。（备注：提供相关技术参数佐证材料，如第三方检测报告或厂家检测报告或产品说明书或产品彩页或官网介绍截图等内容，并加盖供应商公章，予以证明其技术参数的响应性，未提供相关证明材料，该项不得分。）	15.0000	客观	租赁设备说明一览表 服务内容及服务要求 应答表 服务方案
	非标▲技术参数	根据投标人对技术要求中基础安全防护服务标注“非标▲”的技术响应情况赋分： 1. 技术参数满足项目需求，得 10 分； 2. 技术参数负偏离未超过 10 项，得 5 分； 3. 技术参数负偏离超过 10 项（含 10 项），得 0 分。	10.0000	主观	服务方案 租赁设备说明一览表 服务内容及服务要求 应答表

详细评审

服务方案	根据投标人提供所需的总体服务方案，包括但不限于①基础安全防护服务方案②安全运维方案③安全管理体系服务方案④基础安全防护服务交付物服务方案⑤安全运维服务交付成果服务方案⑥安全管理体系服务交付物服务方案等方面赋分： 1. 服务方案紧密贴合工作实际需求，内容详尽全面，服务描述条理清晰，针对性极强，完全符合项目要求，得 5 分； 2. 服务方案符合工作基本要求，整体框架较为完备，服务内容阐述较为明确，与项目需求保持一致，得 3 分； 3. 服务方案与工作需求存在出入，完整性有待提升，服务内容描述不够详尽，未能充分满足项目要求，方案不具体或存在漏项，得 2 分； 4. 实施方案存在严重缺陷，得 1 分。 5. 未提供相关说明，得 0 分。注：每个方案满分 5 分，共 30 分。	30.0000	主观	服务方案
服务保障	根据投标人提供针对本项目服务保障方案（包括但不限于项目组织、人员分配、进度保障）等方面赋分： 1. 方案措施科学、合理、针对性强，完全满足项目要求，得 5 分； 2. 方案措施较合理、能满足项目要求，针对性基本符合项目要求，得 3 分； 3. 方案措施不合理，无针对性措施，得 1 分； 4. 未提供相关说明，得 0 分。	5.0000	主观	服务方案

团队人员	<p>根据投标人拟投入本项目的团队人员配备情况进行赋分： 1.拟担任本项目的项目负责人具有信息系统项目管理师证书或PMP（项目管理专业人士资格认证）证书，得1分；</p> <p>2.拟担任本项目的技术总监具有信息系统项目管理师证书或PMP（项目管理专业人士资格认证）证书，得1分； 3.团队成员中（项目负责人和技术总监除外）具备：①CISP（注册信息安全专业资格认证证书）；②CISSP（信息系统安全专业认证证书）；③PMP（项目管理专业人士资格认证证书）；④信息系统项目管理师证书；⑤系统集成项目管理工程师，每提供一个，得1分，共5分。注：同一人具有多个证书只按一个计算。</p>	7.0000	客观	服务方案
质量保证	<p>根据投标人针对本项目的质量保障情况内容赋分： 1.保证方法及措施内容全面详细，科学合理、针对性强，得5分； 2.保证方法及措施内容全面，但部分内容描述不够详细，基本符合项目需求，得3分； 3.保证方法及措施内容不完整，不符合项目需求，得1分； 4.未提供相关说明，得0分。</p>	5.0000	主观	服务方案
应急预案	<p>根据投标人针对本项目实施过程中可能出现的问题提供的应急预案详述，应急工作流程，应急措施等应急预案及措施等具体内容赋分： 1.方案内容完整科学，符合项目实际及需求，得4分； 2.方案内容完整，基本符合项目实际需求，得3分； 3.方案内容不完整，不符合项目实际需求，存在瑕疵，得1分； 4.未提供相关说明，得0分。</p>	4.0000	主观	服务方案

	售后服务承诺	根据投标人的本地化售后服务承诺、维护保修计划，包括但不限于售后服务内容、响应方式、响应时间、故障服务管理、问题管理、设备返修管理、服务报告管理等方面赋分： 1. 售后服务措施和承诺详细可行，操作性强，得 5 分； 2. 售后服务措施和承诺基本满足项目需求，具有一定操作性，得 3 分； 3. 售后服务措施和承诺不符合项目需求，得 1 分； 4. 未提供相关说明，得 0 分。	5.0000	主观	服务方案
	同类业绩	投标人 2022年1月1日 至今具有同类项目业绩（以合同为准，包含合同首页、关键内容页及签署页），每提供 1 份得 2 分，满分 4 分。	4.0000	客观	服务方案
价格分	价格分	评分方法： $P=10 \times P_{min}/P_n$ 其中： P_{min} ：合格供应商投标报价中的最低价。 P_n ：第 n 个合格供应商的投标报价。	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

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 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	--------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------

采购包2：

评审因素		评审标准			
分值构成		详细评审90.00分 报价得分10.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	监理实施方案	根据投标人提供监理实施方案，包括但不限于①监理总体的工作目标②监理内容③服务方式④监理流程等方面赋分：描述全面、合理，符合项目特点。以上内容完整、合理、不存在瑕疵，得8分；每缺一项扣2分，存在瑕疵的一项扣1分，扣完为止。（本项所指“瑕疵”是指内容不完整或缺少关键点；非专门针对本项目或不适用本项目特性、套用其他项目内容；存在逻辑漏洞、科学原理或常识错误；不利于本项目实施、现有技术条件下无法实现等任意一种情形）。	8.0000	主观	服务方案 服务内容及服务要求 应答表
	质量控制管理措施	根据投标人对本项目的质量控制管理措施方案进行赋分：1.质量控制管理措施方案明显高于相关行业标准的，得10分；2.质量控制管理措施方案详细完整、科学合理，适用于本项目，得8分；3.质量控制管理措施方案具备整、科学合理，基本适用于本项目，得5分；4.质量控制管理措施方案不完整、安排合理，不适用于本项目，得1分；5.未提供相关说明，得0分。	10.0000	主观	服务方案
	进度控制管理措施	根据投标人对本项目制定的进度管理及管控措施方案赋分：1.进度计划、时间节点及工作内容等安排详细合理，有细化措施等内容，得8分；2.进度计划、时间节点及工作内容安排详细，措施内容基本可行，得6分；3.进度安排、工作计划与进度安排相关措施具备，得4分；4.进度计划、时间节点及工作内容安排粗略，措施内容粗略，得2分。5.未提供相关说明，得0分。	8.0000	主观	服务方案

变更控制的方法和措施	根据投标人对运维服务（SLA）变更的监管控制方案赋分： 1.变更控制的方法和措施，内容详细、规范、可行性强，得6分； 2.变更控制的方法和措施，内容基本完整、较为规范，具有可行性，得4分； 3.变更控制的方法和措施，内容不完整或可行性一般，得2分； 4.未提供相关说明，得0分。	6.0000	主观	服务方案
投资控制的方法和措施	根据投标人对项目投资控制方法和措施等方面赋分： 1.投资控制的方法和措施，内容详细、规范、可行性强，得6分； 2.投资控制的方法和措施，内容基本完整、较为规范，具有可行性，得4分； 3.投资控制的方法和措施，内容不完整或可行性一般，得2分； 4.未提供相关说明，得0分。	6.0000	主观	服务方案
信息安全控制措施	根据投标人对项目实际情况，提供信息安全控制措施，项目信息安全和施工安全控制措施满足项目要求和信息安全标准，符合项目特点等方面赋分： 1.信息安全控制措施，方案详细、规范、可行性强，得6分； 2.信息安全控制措施，方案基本完整、较为规范，具有可行性，得4分； 3.信息安全控制措施，方案内容不完整，得2分； 4.未提供相关说明，得0分。	6.0000	主观	服务方案

详细评审	合同和文档管理的措施	根据投标人对项目合同和文档信息管理的内容完整、明确；方法和措施、流程合理可行，符合项目特点，满足项目运维和项目审计的需要等方面赋分： 1.合同文档管理措施 ，方案详细、规范、可行性强，得 5分 ； 2.合同文档管理措施 ，方案基本完整、较为规范，具有可行性，得 3分 ； 3.合同文档管理措施 ，方案内容不完整或可行性一般，得 1分 ； 4.未提供相关说明 ，得 0分 。	5.0000	主观	服务方案
	组织协调的方法和措施	根据投标人对项目组织协调的方法和措施合理可行，流程规范，保证各相关方的良好沟通和无缝衔接，保证项目相关信息传递的及时性和有效性等方面赋分： 1.方法措施 详细、规范、可行性强，得 5分 ； 2.方法措施 基本完整、较为规范，具有可行性，得 3分 ； 3.方法措施 内容不完整或可行性一般，得 1分 ； 4.未提供相关说明 ，得 0分 。	5.0000	主观	服务方案
	保密措施	根据投标人对项目安全保密职责，提供具体的保密措施等方面赋分： 1.保密措施 内容详细完整，能够提供保密承诺，且保密措施利于项目实施，得 5分 ； 2.保密措施 内容基本满足本项目需求，未提供保密承诺，但不影响项目实施，得 3分 ； 3.保密措施 内容有缺陷，影响到项目实施，得 1分 ； 4.未提供相关说明 ，得 0分 。	5.0000	主观	服务方案

合理化建议	根据投标人对项目采购需求及项目实际情况，能够提出有价值的合理化建议，且具体切实可行，有利于提升本项目整体服务质量等方面赋分：1.建议合理、切实可行，内容详尽、全面，得3分；2.建议较合理、可行，内容较详尽、全面，得2分；3.内容粗略，建议不合理、可行性一般，得1分；4.未提供相关说明，得0分。	3.0000	主观	服务方案
企业情况	投标人具有信息系统工程监理服务标准贯标证书的，得2分，未提供得0分。	2.0000	客观	服务方案
企业资信	投标人具有ISO27001信息安全管理体系认证证书、IS20000信息技术服务管理体系认证证书，认证范围须包含“信息系统工程咨询、监理及相关技术服务”。每提供1个得1分，最高得2分。未提供不得分。	2.0000	客观	服务方案

监理团队	<p>项目监理团队配备项目总监理工程师1名，项目总监理工程师代表1名，专业监理工程师3名人员，在具备“信息系统监理工程师资质”（提供证书）基础上：一、总监理工程师1.具有信息系统项目管理师证书，得1分；2.具有系统架构设计师证书，得2分；3.具有软件工程造价师证书，得1分；4.具有信息安全工程师证书，得2分；5.近3年（2022年1月至今）类似项目合同业绩证明材料，每提供1份得1分，最多得2分。（注：附完整业绩合同并加盖供应商公章，业绩证明材料需体现项目总监理工程师姓名。）</p> <p>）注：提供2025年供应商为其缴纳的至少3个月的社保缴纳证明扫描件，未提供不得分。二、总监理工程师代表1.提供信息系统项目管理师证书及系统集成项目管理工程师证书，每提供1个得1分，最多得2分。注：提供2025年供应商为其缴纳的至少3个月的社保缴纳证明扫描件，未提供不得分。三、专业监理工程师1.提供软件测试工程师证书、信息系统项目管理师证书、一级建造师（机电）证书、IT服务项目经理证书，每提供1个得1.5分，最多得6分。注：提供2025年供应商为其缴纳的至少3个月的社保缴纳证明扫描件，未提供不得分。</p>	16.0000	客观	商务应答表 服务方案
------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------	----	---------------

	团队架构	项目监理团队配备专业监理工程师，满足本项目采购需求中人员配备要求，项目团队结构合理、分工明确、技术能力强，具有相关资格证书等方面赋分： 1. 项目团队人员充裕，分工明确，配备合理，得 2 分； 2. 人员基本满足要求，职责较为明确，配备一般，得 1 分； 3. 未提供不得分。	2.0000	主观	服务方案
	业绩	投标人 2022 年 1 月至今具有同类项目业绩（以合同为准，包含合同首页、关键内容页及签署页），每提供 1 份得 2 分，满分 6 分。	6.0000	客观	服务方案
价格分	价格分	评分方法： $P=10 \times P_{\min} / P_n$ 其中： P_{min} ：合格供应商投标报价中的最低价。 P_n ：第 n 个合格供应商的投标报价。	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
无					

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的证明材料须清晰可辨。

（最低评标价法适用）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倾向性和歧视性、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）评标前，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）评标过程中，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）评标过程中，不得干预或者影响正常评标工作，不得发表倾向性、引导性意见，不得修改或细化招标文件确定的评标程序、评标方法、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标意见，不得拒绝对自己的评标意见签字确认。

（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，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6章投标文件格式

6.1 投标文件封面格式

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: 开标一览表

详见附件: 分项报价表

详见附件: 标的清单

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: 资格证明文件

详见附件: 租赁设备说明一览表

详见附件: 商务应答表

详见附件: 服务内容及服务要求应答表

详见附件: 服务方案

采购包2:

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: 开标一览表

详见附件: 分项报价表

详见附件: 标的清单

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: 资格证明文件

详见附件: 商务应答表

详见附件: 服务内容及服务要求应答表

详见附件: 服务方案

第7章 拟签订采购合同文本

详见附件：合同文本.docx

