

招 标 文 件

(服务类)

采购项目名称: 2026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: HZGH-2026-058

西安市数据局

华招广和项目管理有限公司共同编制

2026年08月07日

第一章 投标邀请

华招广和项目管理有限公司（以下简称“代理机构”）受西安市数据局委托，拟对2026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：HZGH-2026-058

二、采购项目名称：2026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

西安市数据局2026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，分为两个采购包，（包1：安全运维服务）项目服务范围涵盖网络安全防护、安全运维、终端准入认证及安全检测等服务。（包2：信息化工程监理服务）对项目服务质量、项目投资、项目实施过程进行控制，对整个项目进行监管。具体服务内容包括项目管理、项目实施管理、项目风险评估与控制等监理服务。具体服务内容及需求详见本项目招标文件。

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（信息化工程监理服务）：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、主体资格：供应商为向招标人提供相关服务的法人或其他组织；

2、信用要求：供应商未被“信用中国”网站列入“重大税收违法失信主体名单”；未被“中国执行信息公开网”列入“失信被执行人”；未被“中国政府采购网”网站列入“政府采购严重违法失信行为记录名单”；未被“国家企业信用信息公示系统”网站“列入严重违法失信名单（黑名单）信息”；

3、财务报告：供应商提供2025年度经审计完整的财务审计报告（成立时间至提交响应文件截止时间不足一年的可提供自成立以来的资产负债表）或在开标日期前六个月内其基本开户银行出具的资信证明。

4、社保的缴费证明材料：提供递交响应文件截止时间前一年内至少一个月已缴纳的社会保障资金的凭据（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供应商应提供相关文件证明；

5、纳税的缴费证明材料：供应商递交响应文件截止时间前一年内至少一个月依法缴纳税收的相关凭据（时间以税款所属日期为准，税种须包含增值税或企业所得税，凭据应有税务机关或代收机关的公章或业务专用章）；其他组织和自然人提供缴纳税收的凭据；依法免征、零申报的供应商应提供相关文件证明材料。

采购包2：

1、主体资格：供应商为向招标人提供相关服务的法人或其他组织；

2、信用要求：供应商未被“信用中国”网站列入“重大税收违法失信主体名单”；未被“中国执行信息公开网”列入“失信被执行人”；未被“中国政府采购网”网站列入“政府采购严重违法失信行为记录名单”；未被“国家企业信用信息公示系统”网站“列入严重违法失信名单（黑名单）信息”；

3、财务报告：供应商提供2025年度经审计完整的财务审计报告（成立时间至提交响应文件截止时间不足一年的可提供自成立以来的资产负债表）或在开标日期前六个月内其基本开户银行出具的资信证明。

4、社保的缴费证明材料：提供递交响应文件截止时间前一年内至少一个月已缴纳的社会保障资金的凭据（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供应商应提供相关文件证明；

5、纳税的缴费证明材料：供应商递交响应文件截止时间前一年内至少一个月依法缴纳税收的相关凭据（时间以税款所属日期为准，税种须包含增值税或企业所得税，凭据应有税务机关或代收机关的公章或业务专用章）；其他组织和自然人提供缴纳税收的凭据；依法免征、零申报的供应商应提供相关文件证明材料。

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。

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：西安市数据局

地址：西安市未央区凤城八路109号

邮编：710000

联系人：西安市数据局基础设施处张工

联系电话：67095503

代理机构：华招广和项目管理有限公司

地址：陕西省西安市雁塔区南二环中段西部国际广场B座28层2803室

邮编：710000

联系人：王佳

联系电话：18829685840

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）	本项目各包采购预算金额如下： 采购包1：11,391,944.00元 采购包2：208,336.00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 采购包2：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 采购包2：不接受 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。 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.本项目采购无产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。 3.本项目采购无产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购无产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/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 采购包2：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 代理服务收费标准：参照《代理服务收费管理暂行办法的通知》(计价格[2002]1980号)、《关于招标代理服务收费有关问题的通知》(发改办价格(2003)857号)以及《关于降低部分建设项目收费标准规范收费行为等有关问题的通知》(发改价格(2011)534号)规定的标准，优惠后按照定额收取。包1：代理服务费：44000.00元 包2：代理服务费：2500.00元
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，采购人将政府采购合同报本级财政部门备案。
19	进口产品	不允许
20	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
21	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。
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西安市数据局和华招广和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，评标细则及标准由西安市数据局负责解释。除上述招标文件内容，其他内容由华招广和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华招广和项目管理有限公司。

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的所有的事项、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、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：

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，招标人享有使用权（含招标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。

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。

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：

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：

详见合同约定

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）

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 华招广和项目管理有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由华招广和项目管理有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 华招广和项目管理有限公司 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)；
(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：王佳

联系电话：18829685840

地址：陕西省西安市雁塔区南二环中段西部国际广场B座28层2803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)。

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

西安市数据局2026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，分为两个采购包，（包1：安全运维服务）项目服务范围涵盖网络安全防护、安全运维、终端准入认证及安全检测等服务。（包2：信息化工程监理服务）对项目服务质量、项目投资、项目实施过程进行控制，对整个项目进行监管。具体服务内容包括项目管理、项目实施管理、项目风险评估与控制等监理服务。具体服务内容及需求详见本项目招标文件。

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）：11,391,944.00
采购包最高限价（元）：11,391,944.00
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	2026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	11,391,944.00	项	软件和信息技术服务业	否	否	否	否	否

采购包2：
采购包预算金额（元）：208,336.00
采购包最高限价（元）：208,336.00
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	2026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 监理服务	1.00	208,336.00	项	软件和信息技术服务业	否	否	否	否	否

3.2.2服务要求

采购包1：

序号	参数性质	技术参数与性能指标																
		1.基础安全防护服务 基础安全防护服务主要内容包括网络安全防护、安全监管控制服务。 特征库或版本升级要求 要求对特征库类设备要及时获取最新的特征库和软件版本信息，并根据厂商发布的安全补丁和功能进行更新。 设备要求 本次服务设备均采用软硬一体设备或硬件设备，并定期对现有设备进行评估，确定是否需要更新替换，评估因素包括设备的性能、接口等因素； 根据业务需求和技术发展趋势，评估适合的设备型号和技术。提供详细的设备更换服务方案，要有详细的设备更新替换规划，包括更新的时间表、备用方案等。更换规划要充分考虑电子政务运行稳定状况，确保设备更新替换工作能够有序进行。 兼容性要求 确保新设备与其他设备、系统和业务的兼容性。更换设备前，要进行充分的兼容性测试，包括硬件接口兼容性、软件协议兼容性等。 国产化要求 要求项目中涉及的设备搭载的操作系统和芯片均需符合国产化要求。 其他要求 服务期终止后，服务商应保障服务顺利衔接过渡，不得无故拖延或拒履义务。 服务内容清单 <table><tr><th>序号</th><th>一级服务内容</th><th>二级服务内容</th><th>服务要求</th><th>服务支撑工具/设备数量</th><th>服务周期(月)</th></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>					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)						
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)													

			入安全防护服务			
		2	态势感知 探针服务	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。 2.支持双向检测事件库≥20000个； 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SSL 3.0, TLS1.0/1.1/1.2； 4.持基于工具特征的WEBSHELL检测:如冰蝎连接； 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； 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；	1	12

[illegible]

		5	防火墙服务	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。 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。	2	12
--	--	---	-------	---	---	----

6		负载均衡服务	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。 2.支持透明、路由、混合及单臂、三角传输模式部署 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。 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； 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。 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； 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。	2	12
		运营商机抗DDoS服务	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； 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； 3.防护IP地址256个以内；DNS 解析不做变更，用户端零操作；	2	12

12	政务云平台（凤八）安全防护服务	防火墙服务	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。 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。	2	12
----	-----------------	-------	---	---	----

13	政务云平台（西咸）政务外网侧安全防护服务	防火墙服务	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。 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。	2	12
----	----------------------	-------	---	---	----

14		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， QinQ等功能。	2	12
----	--	-------	---	---	----

		15	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；SSD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。 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。	2	12
--	--	----	--	---	----

		18	全流量分析服务	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≥64G；网络流量处理能力≥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≥50TB/秒。 2.存储硬盘不少于20T； 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； 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； 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； 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）；	1	12

20	云外数据中心托管区安全防护服务	入侵防御系统服务	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≥100Gbps，最大并发连接数≥2000W，每秒新建HTTP连接数≥50W。 2.系统应支持网线模式部署和透明多口桥部署； 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； 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。 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。	2	12
----	-----------------	----------	--	---	----

1		21	Web应用 防火墙服 务	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。 2.支持透明模式、代理模式同时部署方式。 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； 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 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；	2	12

		24	威胁感知服务	1.服务期内以威胁情报驱动，为整体网络安全运维服务提供威胁情报支撑平台工具/设备，内容包括情报概览、情报分类统计、情报查询/命中情况、重大安全事件、热点情报狩猎等。 2.支持代理网环境下的互联网情报源接入和情报查询。 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。 4.支持以web查询或API接口查询的方式，查询漏洞情报； 5.支持展示多源情报查询结果和历史情报查询信息； 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； 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。	1	12
			核心交换区（流量			

			镜像分析 ）安全防护服务			
		25		全流量分析服务	1	12

26	政务专网 局域网区 (市政府 、市委、 综合楼) 安全防护 服务	防火墙服 务	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，应配备冗余电源；千兆电口≥ 10个，千兆光口≥ 4个，万兆SFP+接口≥ 8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。 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； 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； 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； 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。	6	12
----	--	-----------	---	---	----

			入安全防护服务		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，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≥40 Gbps，最大并发连接数≥400万，每秒新建连接数≥10万。 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； 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； 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； 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。	2	12

		31	日志审计服务	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，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。 2.支持SNMP Trap、Syslog、ODBCJDBC、文件\文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC等多种方式完成日志收集功能； 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； 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； 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	1	12
--	--	----	--------	---	---	----

32	数据交互 区安全防 护服务	数据交换 系统服务	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。 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。 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； 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。	1	12
----	---------------------	--------------	---	---	----

		33	防火墙服务	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。 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； 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； 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；	1	12
		34	数据镜像交换机服务	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。 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）。	1	12
				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/		

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

			36	网站监测服务	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。 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； 3.支持Ping、HTTP、GET请求等网站安全监控功能； 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； 5.支持自定义监测周期对网页挂马进行实时监测； 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。	1	12

			37	日志审计服务	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。 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； 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； 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； 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；	1	12

					，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。 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； 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； 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。 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。 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； 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		
		39	态势感知服务			1	12

				信、启明星辰、网御星云等。 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； 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		
				国产化平台SDP控制器，标准2U机箱，冗余电源；内置国家密码局检测通过的国家商用密码卡；标准配置6个10/100/1000M Base-TX;4个SFP千兆光口；2个扩展槽位；标准配置16G内存，系统盘128G，存储盘4T硬盘；支持并发用户数8000个；支持与SDP安全网关和客户端组合联动实现网络隐身的功能，确保只有通过认证的主体才能接入SDP安全网关；支持多因素身份认证，包括口令、证书、动态令牌、UKEY等多种认证方式灵活组合，支持基于国密SM2算法的数字证书的身份认证，支持基于LDAP、Radius、CAS、Oauth协议标准的第三方认证平台；能够联动SDP安全网关对不符合安全策略的接入主体进行权限限制或强制下线等处置动作。	2	12

					国产化平台SDP网关，标准2U机箱，交流冗余电源；内置国家密码局检测通过的国家商用密码卡；标准配置6个10/100/1000M Base-TX, 4个千兆光口，2个扩展卡槽位；明文整机吞吐35G，国密加密吞吐量1500M；128G系统盘；支持SM1、SM2、SM3、SM4等国家商用密码算法；可集群方式实现横向扩展。支持与SDP控制器和客户端组合联动实现网络隐身的功能，确保只有通过认证的主体才能接入SDP安全网关，SDP安全网关不响应未通过认证主体的连接请求；支持基于国密算法的传输加密，实现SDP安全网关和客户端之间数据传输的机密性及完整性保护；支持被保护资源的地址隐藏；支持与SDP控制器联动，含并发3000授权（移动端和PC端）。	2	12

		41	蜜罐服务	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能力。 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。 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； 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； 5.支持数据库类蜜罐，包括但不限于：Mysql、Mysql溯源、PostgreSQL、redis； 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、Ftp、Xshell、Windows凭据、RDP远程登录；	1	12
		2.终端准入认证服务	服务内容			
		提供用户终端授权数量≥10000点的服务，服务内容包括400热线服务、一般问题现场支持服务、紧急故障现场支持服务、根因分析服务、问题管理服务、终端环境软件适配服务、主动式系统健康巡检服务、服务运维报告等。				

服务要求

400热线服务	服务时间：7X24；响应时间： ≤30min
一般问题现场支持服务	按需提供一般问题故障（主要IT设施轻微损坏，不影响正常办公周边业务功能不可用，不影响用户正常使用； 因系统平台异常，影响用户正常办公不超过 4 小时不影响项目关键节点进度推进）处理现场支持服务；到达现场时间： ≤24h；
紧急故障现场支持服务	按需提供紧急故障（主要 IT 设施遭受严重损坏，或系统平台出现严重异常，无法在短时间内恢复。核心业务重要功能不可用且大面积影响用户；因系统平台异常，大面积影响用户正常办公超过 8 小时项目进度完全中断，严重影响客户关系）现场支持处理服务；达到现场时间： ≤4h；
根因分析服务	在紧急故障发生后，由技术专家定位到隐藏在表面问题之下的根本原因，并从根源上解决问题避免问题再次发生。对于无法避免的问题提供应急处理方案消除、降低后续相关故障影响。最终通过报告的形式提交客户；
问题管理服务	提供专属服务经理的角色统筹客户的问题管理、需求管理、改进建议等单一紧急事件问题处理反馈时间≤2h，其他时间当天同步；多问题每周提供问题分析报告；
终端环境软件适配服务	除了常规的技术支持以 外，为了应对由于终端环境的复杂性以及终端环境改变造成系统安全保障功效 降低，需要结合研发人员持续投入去适配终端环境；例如客户端的兼容性适配 （软件冲突）、系统驱动插件适配、第三方软件更新造成管控审计异常等。
主动式系统健康巡检服务	安排现场服务顾问到客户现场对系统的运行、使用情况、风险隐患等进行检 查和改进并提交巡检报告和改进建议
服务运维报告	按需提供月、年度服务报告，总结客户年度稳定性服务项及重大项目成果。

3.统一安全运维服务

3.1一体化安全运维平台服务

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、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。 2、服务内容 安全管理制度知识库功能包括：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。 1) 知识库归类设置 需设置哪些知识库文档为必须上传。 2) 知识文档上传 格式支持pdf、doc、xls、wps等，同时支持视频文件上传。 3) 知识文档审核 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。 4) 知识库综合查询 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。 5) 文档管理功能 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。		
	1	安全管理制度知识库		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。 2、服务内容 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。		

				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。 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。 3) 日志管理 记录所有访问日志，确保可以追溯每个访问行为，并定期审查访问日志以及及时发现和处理异常访问行为。 4) 绩效评估 服务中需要有明确的网络安全工作绩效指标，如安全漏洞发现数量、安全事件响应时间、安全策略执行情况等。 定期收集和统计人员的工作数据，根据绩效指标进行量化评估，生成绩效报告，并上传至平台。 绩效评估结果与薪酬调整、晋升、奖励等挂钩，激励人员积极工作，提高工作质量和效率。 5) 安全意识教育 提供西安市数据局网络安全、人员安全的相关规定，应急响应与安全事件处置流程，供人员自主学习。		
		2	人员管理			

		3	业务系统全生命周期安全管理	1、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。 2、服务内容 1) 等保管理 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。 2) 备案管理 有效管理等保系统的定级备案情况，对备案证明等相关材料进行管理，支持对已备案、已测评、已过期等信息进行统计，支持定级备案的高级搜索。
				1、服务范围 需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。 2、服务内容 1) 信息共享与沟通协作 打破信息孤岛，实现各参与方之间网络安全事件信息、处置经验等的实时共享和快速传递，还提供即时通信、邮件通知、公告发布等多种沟通方式，方便各方及时交流。 2) 事件监测与预警 通过部署在网络中的各类传感器、监控设备等，实时收集网络流量、系统日志等信息，利用大数据分析、机器学习等技术对收集到的数据进行深度分析和关联挖掘，及时发现潜在的网络安全威胁和异常行为，并发出预警。 3) 应急管理 在网络安全事件发生时，明确各参与方的职责和任务，制定详细的处置流程和应急预案，根据事件的严重程度和发展态势，及时调整处置策略和资源配置，协调各方力量进行应急处置。 4) 协同处置 在重大突发事件处置时，各厂家将监测数据

					上传至协同处置，进行集中分析和处理。能够根据事件现状影响快速制定动态处置流程。 5) 流程管理 对网络安全事件的处置过程进行全程跟踪和记录，包括事件的上报、受理、指派、处理、反馈、审核等环节，确保处置流程的规范化和标准化，同时支持对处置流程进行自定义和优化。 流程管理模块为用户提供灵活的流程管理，用户可以根据自身的需要创建应用，自定义表单，自定义流程中的各种不同类型的节点（如人工任务，人工审批，并行网关，抄送任务等），各节点用户均可根据需要自由配置处置人员，也可自动分配选定角色或组织下的人员。 6) 资源管理与协调 对参与网络安全协同处置的各方资源进行统一管理和协调，包括人员管理、流程管理等，实现各方资源的合理分配和高效利用，提高协同处置的效率和效果。 7) 重大保障 实现重大保障任务的管理，可新增、下发具体的重大保障任务，实现该重大保障任务的全过程管理，查询重大保障任务的执行情况，包括：备战阶段、临战阶段、实战阶段、总结阶段的人员安排及报告信息。 提供排班管理模块，实现重大保障期间人员值守安排和值班管理工作，主要包括班次管理、班组管理、排班管理、值班日报等。 8) 专项任务 主要支持对安全运维体系开展的各类日常、周期性的安全运维工作进行管理，包括周期性的测试任务、工单分配等工作，可以定义任务的开展流程，包括任务名称、任务流程等信息，查询任务当前的执行状态。支持运维工作中工单分配的创建、审批、挂起、导出等功能。 9) 风险通知 安全管理人员或应急响应团队成员根据实际		
--	--	--	--	--	--	--	--

				1、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。 2、服务内容 1) 网络安全拓扑图 实现拓扑图的动态绘制与管理，支持自定义绘制。 2) 监控探针 针对政务云的网络设备、安全设备、主机设备等目标对象，能够提供相应的探针实现系统的性能指标信息的采集。 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。 4) 资产管理 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。 5) 设备监控 实现针对专用计算机软硬件环境以及提供设备的资产维护信息，包括品牌、型号、存放地点、资产状态、资产归属等。 6) 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。 7) 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、告警级别提升管理功能，需提供告警集中、告警恢复、告警关闭功能。
	5	安全运维管理		1、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。

2、服务内容

1) 文档管理

对项目重要文档进行管理，功能主要有项目文档上传、项目文档审核及项目文档查询。可创建项目文档信息，上传项目文档附件，同时需设置可查阅人员权限，精确到人。实现项目文档的规范化、版本化管控。

系统需提供文档列表展示页面，呈现文档版本、类型、内容、附件、描述及说明等信息，支持关键词筛选查询，同时提供新增、复制、导入、导出等批量操作功能，满足文档数据高效维护需要。

2) 计划管理

实现项目周期计划的管控。系统需提供计划列表展示页面，按项目分组呈现计划名称、关联项目、起止时间、描述及说明等信息，支持关键词筛选查询，同时提供新增、复制、导入、导出等批量操作功能，满足计划数据高效维护需求。

同时需提供计划详情编辑页面，支持计划起止时间选择、描述录入及副文本格式的说明编辑；配套计划条目列表与相关文档子模块，可精细化管理子计划名称、时间节点、交付物及关联文档，实现项目计划精细化拆解管理。

3) 会议管理

实现会议从创建、执行到归档的信息化管控。系统需提供会议列表展示与查询功能，清晰呈现会议名称、主题、主要议题、主持人、类型、召开方式、地点、状态及计划或实际时间等核心信息，支持按关键词筛选、批量新增、复制、导入与导出操作，满足会议数据的高效管理。

4) 项目信息

实现项目核心数据的集中化管理。系统需提供项目列表展示页面，清晰呈现项目名称、编号、项目经理、类型、状态、预算金额、招标日期、中标金额、中标方、计划工期等核心信息，支持关键词筛选查询，同时提供

	心指标的直观感知。 模块需包含核心指标统计区，展示项目总数、进行中、已完成、已暂停项目数量，直观反映项目整体规模与运行态势。 10) 业务配置 系统需提供相关单位信息，清晰展示关联项目、单位名称、单位角色、描述及说明等信息，支持通过新增、复制、导入、导出功能批量维护单位数据，明确如“甲方”等单位参与项目的角色定位。	
--	--	--

		7	安全设备策略备份	1、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。 2、服务内容 提供针对安全设备策略的备份与管理服务。 实现不同设备策略备份目录的快速查询，确保在设备故障、策略误操作或遭遇安全事件后，能迅速找到对应设备的备份策略，保障政务业务的连续性与安全性。服务范围涵盖项目中部署的安全设备，包括但不限于防火墙、入侵防御系统、Web应用防火墙等设备的配置文件与安全策略。 提供备份策略登记功能，支持备份策略的上传、下载、重命名、删除操作。 提供设备管理备份策略，支持按备份时间查找备份策略。 提供设备策略管理功能，可依据设备所在区域和设备类型进行设备的登记、删除、查询操作。 提供按设备查看备份策略功能，可按设备所在区域和设备类型搜索设备备份策略。 提供历史备份策略管理服务，支持保留历史备份，具备备份日志记录功能； 提供备份策略分类功能，可对备份策略进行分类管理，上传备份策略时可选择策略类别；备份策略类别不少于三种，包括但不限于配置备份、剧本备份、规则库等。 提供备份策略导出功能，可按照区域、设备、时间段对备份策略进行导出；支持备份策略统计功能，可统计当前备份策略总数、备份策略按月分布情况等。	
--	--	---	----------	--	--

		3.2安全运维服务 3.2.1日常运维服务 服务内容 安全运维平台维护 1) 安全管理制度知识库：每周收集最新的安全法规、行业标准和内部安全管理体系，及时更新安全制度知识库，确保知识的时效性。每月对知识库中的所有文档进行准确性和完整性审核，纠正错误信息，补充缺失内容。 2) 人员管理：实时更新各厂商运维人员的岗位变动、权限变更等信息，确保系统中运维人员信息的准确性和一致性，并定期清理离职员工的账号，确保系统安全。根据业务需求和安全策略，及时调整用户权限，并每月定期审核用户权限设置，确保用户权限与岗位职责相符，避免权限滥用。 3) 协同处置：每日对系统内的即时通讯与公告发布功能展开细致检查，全方位确保消息发送与接收具备高度的及时性和准确性。在日常运行过程中，不定期对系统内发现的网络安全威胁和异常行为进行预警并协调各服务商按照制定详细的处置流程和应急预案进行系统处置。重大保障时期实施全流程精细化管理，涵盖任务部署、执行监督、问题处理等各个环节，确保业务系统在重保时期能够安全、稳定、高效地运行。 5) 安全运维管理：针对网络安全拓扑图进行及时更新并实时监控资产状态，确保资产准确及数据支撑可靠；定期检查告警中心各项服务与功能，保障运维服务操作入口顺畅。 6) 安全服务管理：定期审核项目文档上传，保障项目文档管理有序，并对项目管理文档进行归类；审核填写的项目问题、验证处理结果并查询问题；实时监控项目任务状态、进度、逾期等各项数据。保障系统各功能稳定运行。 (2) 各服务商的协调统筹 全面收集各服务商运维人员的详细联系方式，确保在任何紧急或日常情况下，都能迅速地联系到各服务商相关人员。一旦应急事件发生，需迅速启动协调机制，依据应急预案精准地向各服务商传达指令，确保各服务方清楚知晓自身任务与行动方向；在应急响应结束后，组织各服务商进行全面总结，共同探讨在此次事件中遇到的问题、取得的成效以及需要改进的地方，不断提升应对各类应急事件的能力。 (3) 日常工单处理 及时响应下发的工单，并在规定时间内对其需求进行分析并处理，工单完成后需及时通知委办局进行业务验证。针对无法完成的工单需向委办局详细说明理由。 质量要求：日常运维人员需具备丰富的网络安全领域经验，熟悉常见网络安全设备

和系统的配置、管理与维护，掌握网络安全技术和工具。同时，应具备良好的沟通能力和团队协作精神，能够与管理方相关部门和人员进行有效的沟通和协作。

日常运维团队管理人员应持有相关的网络安全专业资质证书、云计算相关证书、项目管理证书，以证明其具备相应的专业能力和技术水平。

服务频次：7*24小时（一年）

3.2.2应急响应及处置服务

服务内容

覆盖西安市政务外网网络、市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点）安全平台和业务系统。

（1）应急响应服务内容

根据实际情况，量身定制全面、详细且具有可操作性的应急预案，明确应急响应的组织架构、职责分工、响应流程、处置措施以及资源保障等内容。并且定期对应急预案进行评估和修订，根据业务发展、技术更新以及外部环境变化等因素，及时调整和完善预案，确保其有效性和适应性。

建立实时监测预警机制，运用专业的技术工具和方法，对网络环境、信息系统、业务运行状况等进行实时监测，及时发现潜在的安全威胁和异常情况，并发出预警。

在接到突发事件报警后，按照应急响应预案迅速启动应急响应流程，对事件进行现场勘查和分析，收集相关证据和数据，确定事件的根本原因和影响范围并采取有效的应急处置措施，如隔离受影响的系统或设备、阻断攻击源等，迅速控制事件的发展态势，降低事件造成的损失和影响。

事件处置结束后，对应急响应过程进行全面复盘和总结，分析事件发生的原因、应急响应过程中的优点和不足之处，提出改进措施和建议

3.3.2服务要求

（1）质量要求

运维期间需确保能够从不同维度对各类应急事件进行全面的分析和处理，并熟悉业务特点和应急需求。设备故障类应急响应时间不超过5分钟，恢复时间不超过30分钟。安全入侵事件类应急响应时间不超过5分钟，需查明攻击方法及攻击路径，提供相关日志。

应急响应服务频次：7*24小时响应。

（2）服务工具：自带安全事件监控平台服务工具。

（3）服务方式：一线现场服务和二线线上远程响应相结合。一线远程响应主要负责实时监控、预警发布、初步分析等工作，确保在第一时间发现并响应安全事件；二线现场服务则负责深入排查、修复故障等工作。

3.2.3重大活动保障服务

服务内容

覆盖西安市政务外网网络、市级政务数据中心（凤八节点）、市级政务数据中心（西咸节点）安全平台和业务系统。

（1）重保前：对保障期间所涉及的网络系统、应用程序、服务器等进行全面的安

全评估，包括但不限于漏洞扫描、安全配置检查等，发现潜在的安全风险和薄弱环节。针对结果出具详细的评估报告，明确安全隐患的具体位置、风险程度，并提出相应的整改建议和解决方案。

根据保障活动的特点和安全需求，制定详细的重保方案和应急处置预案，明确各阶段的工作任务、责任分工和时间节点，确保重保工作有序进行。

(2) 重保中：在保障期间，对业务系统、应用程序、服务器等进行7*24小时不间断的实时监控，密切关注系统的运行状态、网络流量、安全事件等并利用专业的网络安全监控工具和技术，对监控数据进行实时分析和预警，及时发现潜在的安全威胁和异常行为。

(3) 重保后：对活动期间的监控数据、安全事件记录、应急响应报告等重要资料进行整理和归档并提交详细的重保工作总结报告，包括重保期间的网络安全状况、应急响应情况和改进建议等内容。

服务要求

- (1) 质量要求：发生重大入侵事件处置响应时间不超过5分钟。
- (2) 服务频次：7*24小时（按需）
- (3) 服务工具：自带所需服务工具。

3.2.4安全监测服务

服务内容

利用态势感知平台，对网络环境进行7*24小时实时监测，持续监控网络流量、系统日志、用户行为等关键信息，及时发现任何异常情况。一旦发现符合预设规则的安全事件或异常行为，平台应立即发出预警通知。预警信息应包括事件的详细描述、发生时间、影响地址、可能的威胁类型等关键信息，以便及时采取应对措施。预警通知方式包括但不限于邮件、短信、即时通讯工具等，确保相关人员能够及时收到通知。

在接收到预警信息后，立即对事件进行初步分析，核实事件的真实性和严重性。通过查看相关的日志数据、流量记录等信息，进一步了解事件的特征和发生过程，判断事件是否为误报或真正的安全威胁。

对于确定为真实安全事件的情况，进行深入的分析和研判。结合网络拓扑结构、业务流程、系统配置等信息，分析事件的来源、攻击路径、可能造成的影响以及潜在的危害程度。确定事件的性质，如是否为恶意攻击、内部违规行为或系统故障等。

利用威胁情报平台，将事件信息与已知的威胁情报进行关联分析。查找是否存在与该事件相关的已知攻击团伙、恶意软件家族或其他威胁信息，获取更多关于事件的背景和相关信息，为事件的应对和处置提供有力支持。

每周需提供一份网络安全事件监测周报，总结本周内监测到的所有安全事件，包括事件的类型、数量、分布情况、处理结果等。每月提供一份月度报告，对本月的网络安全态势进行全面分析，包括安全事件的趋势分析、潜在风险评估以及改进建议等。

服务要求

(1) 人员质量要求：要求现场监测人员服从相关安排，精通网络安全技术，熟悉常见的网络攻击手段和防御方法，能够准确识别和分析安全事件，熟悉本项目所有安全产品的维护管理工作。

(2) 技术质量要求：对在安全监测中监测到的重大的网络安全事件，应在事件发生后5分钟内以口头或书面形式向甲方相关负责人进行实时报告，告知事件的基本情况和初步影响，确保甲方能够及时作出决策。

(3) 服务频次：7*24小时

3.2.5安全通告服务

服务内容

通过多种渠道收集网络安全漏洞信息，包括但不限于官方安全公告、知名安全漏洞平台、安全研究机构报告、行业论坛及社交媒体等，确保获取全面、及时的漏洞资讯。

根据通告接收需求，制定个性化的漏洞通告方案。通告内容应包括漏洞的基本信息（如漏洞编号、名称、发现时间等）、详细描述、影响范围、危害程度、修复建议以及相关参考链接等，确保相关人员能够清晰、准确地了解漏洞情况。

服务要求

(1) 质量要求：要求每周定期提供包括但不限于最新的安全公告，病毒信息，漏洞信息等内容。漏洞从公布到通告不得超过一周。

(2) 服务频次：一月两次。

4.安全检测服务

4.1“三高一弱”服务

服务内容

“三高一弱”检查

围绕互联网区域、电子政务外网区域的指定委办局租户的虚拟机范围，开展“三高一弱”检查，对检测发现的安全问题，按照风险等级（高、中、低）进行分类梳理，形成包含问题详情、影响范围、整改建议的专项检查报告，及时向指定委办局租户及云平台安全管理部门通告。

资产梳理

对检查范围内的所有业务系统资产进行全面摸排，明确资产数量、所属区域、归属租户及责任单位/责任人，建立“资产—区域—租户—责任人”的四维关联关系，形成可视化、可动态更新的“三高一弱”检查资产台账，精准界定后续高风险漏洞、端口、口令等安全检查的范围与对象，为全流程检查工作奠定基础。

高危漏洞检查

针对两大区域所有业务系统开展高危漏洞深度探测，高危漏洞特指存在严重安全风险、易被攻击者利用的软件/系统漏洞，主要包括CVE官方收录漏洞、攻击者高频利用的公开漏洞、0day/1day高危漏洞等。通过工具开展主动探测、全端口扫描，重点检查远程代码执行、数据泄露、拒绝服务、提权攻击、跨站脚本攻击、SQL注入、命令执行等高危漏洞，形成漏洞清单并标注风险等级。具体如下：

风险等级分析：依据漏洞利用难度、危害后果、影响范围，将探测发现的漏洞划分

为高危、中危、低危三个等级，高危漏洞标注核心风险点与潜在攻击路径；

分布特征分析：统计漏洞在两大区域、不同租户、不同资产类型（服务器、数据库、应用系统等）的分布情况，识别漏洞高发区域与资产类型；

成因分析：分析漏洞产生的核心原因，包括系统版本未及时更新、补丁未部署、配置不当、开发规范不达标等，为整改提供针对性方向。

高危端口检查

对两大区域业务系统开放端口进行全面排查，高危端口指存在高危漏洞/弱口令、暴露在公网/政务外网、易被攻击者利用的特定端口。通过工具开展主动端口扫描、端口存活探测、端口服务识别，重点检查业务系统、数据库、中间件、网络设备中易被远程攻击利用、非业务必需且不应暴露的端口，排查端口开放合规性与安全风险。具体如下：

合规性分析：对照云平台端口开放管理规范与政务外网安全要求，判断开放端口是否为业务必需，排查非合规开放、违规暴露的端口；

风险关联分析：将开放端口与高危漏洞、弱口令探测结果关联，分析端口+漏洞/弱口令的组合安全风险，识别易被攻击者突破的端口入口；

分布分析：统计高危端口在两大区域、不同业务系统、不同网络设备中的分布情况，梳理端口开放管理的薄弱环节。

高危行为检查

对两大区域业务系统开展高危行为监测与分析，高危行为包括违规外联、高危攻击行为、异常访问行为、权限滥用行为等。依托现场已有安全设备（防火墙、入侵检测/防御系统、态势感知等），实现对高危风险行为的及时发现、分析与预警通告。具体如下：

行为特征分析：梳理高危行为的发生时间、发起IP、攻击/操作类型、目标资产、行为频次等特征，识别高频高危行为类型；

风险趋势分析：按日/周/月统计高危行为发生数量与变化趋势，分析风险上升/下降的原因，预判潜在安全威胁；

溯源分析：对典型高危行为开展初步溯源，定位行为发起源（内网/外网、特定终端/IP），分析行为背后的潜在意图；

应急处置指导：为责任单位提供高危行为应急处置人工指导，协助采取阻断攻击源、限制访问、恢复系统配置等应急措施，降低安全损失。

弱口令检查

针对两大区域业务系统等各类资产的账号口令开展全面检查，弱口令指易被破解/猜测、复杂性与安全性不足，成为网络攻击主要突破口的密码。

服务通过专用工具开展主动探测、口令爆破、合规性检查，重点覆盖SSH、Ftp、HighGo、WebCAM、REDIS等服务与数据库的口令安全。

服务要求

“三高一弱”服务包括上、下半年各1次政务云上业务系统的安全检测服务，每次安全检

查服务覆盖40余家租户、300余个业务系统及2000余台主机的资产范围，进行高危漏洞排查与修复、高危端口管控、高危行为监测与处置、弱口令治理、检查报告与整改闭环。

服务采用“指定租户主机范围+定向抽查”的组合模式推进“三高一弱”安全检查。检查以各委办局租户虚拟机为核心对象，按互联网区域、电子政务外网区域分类开展抽查扫描，重点推进以下核心任务：工作任务沟通协调、虚拟机租户资产梳理、主机映射策略申请及配置台账梳理、合规漏洞检测覆盖率分析、预警处置全闭环跟踪、整改结果核验等。

其中，资产梳理需覆盖2000余台主机的业务归属、资产名称、部署位置、IP地址及安全状态等核心维度；在策略管理层面，互联网区域“三高一弱”检查需定期申请主机映射扫描策略，并配合完成策略变更、收敛等工作；同时以每50个租户为一组的单元划分标准，建立租户业务定期“三高一弱”检查机制，覆盖资产梳理、策略申请、策略变更、策略回收等全流程。此外，需兼顾业务访问安全与合规要求，防范因策略疏漏引发的扫描盲区或业务中断风险，所有检查操作均安排在非业务高峰期开展。针对电子政务外网业务主机，需申请开通主机安全策略、VPC策略及防火墙策略；针对跨边界设备，需形成完整的策略映射对照清单，同步制定与策略、台账匹配的扫描规则，完成分组下发、分组采集及结果分析等工作。

针对每轮“三高一弱”检查结果，需开展分析与复测，同步跟踪整改报告落地情况，下发整改通知并推动风险闭环管理，形成多轮检查结果的整体分析对比报告，对整改完成情况进行有效性验证。

4.2业务系统上线检测服务

服务内容

针对新上云的政务业务系统上线前安全评估工作，除严格审核业务方提交的安全自查报告等保自评材料等相关安全资料外，还需以提交的材料为基础依据，结合国家网络安全法律法规、政务云安全管理规范、等级保护基本要求等政策标准，综合运用专业技术手段、安全服务工具开展全流程安全评估。

评估工作主要包括：

对业务方提交的全套安全资料进行规范性、完整性、真实性与合规性审核，重点核查资料内容与业务实际情况的一致性；

采用自动化漏洞扫描工具、配置核查工具等开展针对性漏洞检查，识别存在的高危漏洞、中低危漏洞及潜在安全隐患；

依据政务云安全基线、操作系统安全基线、云资源安全配置规范等开展基线核查；开展资料梳理、问题汇总、风险分类，形成标准化核查记录并按要求编写评估报告。

针对评估发现的安全风险与不合规问题，督促业务方完成整改工作，整改完成后开展整改后技术复核与验证核查，确认问题已闭环整改、风险得到有效控制。通过上述全流程工作，全面评估业务系统的安全合规性，最终形成完整、规范、可追溯的正式安全评估报告。

服务要求

按照实际政务云新上线的业务系统数量提供服务，在服务期内达成80个业务系统以上的上线安全检测，形成结果报告。

4.3业务系统下线检测服务

服务内容

资料审核

资料审核是系统下线安全检测的前置环节，审核内容需包括审核下线决策材料、数据迁移或销毁记录，围绕资源回收核查、权限清理验证、网络隔离检查、系统策略配置等关键环节开展全面确认，通过交叉验证确保下线操作落实到位，精准排查并消除潜在安全隐患。确保材料齐全、内容真实、流程合规、审批有效，严禁无审批、违规、缺件下线。

技术核查

围绕资源回收核查、权限清理验证、网络隔离检查、系统策略配置等关键环节开展全面确认，通过交叉验证确保下线操作落实到位，精准排查并消除潜在安全隐患。

报告编写

需规范编制系统下线安全核查报告，形成闭环核查文件，作为系统正式下线、资源归档、责任闭环的核心依据。

服务要求

按照实际政务云下线的业务系统数量提供服务，在服务期内达成20个业务系统以上的下线安全检测，形成结果报告。

4.4大模型、智能体安全风险评估服务

服务内容

提供大模型、智能体安全风险评估服务，在政务领域垂直模型或智能体上线时进行安全风险评估，确保在内容安全、基础环境安全、语料安全等维度符合法律法规及行业规范要求。

评估对象：政务领域垂直模型、智能体。

评估维度：包含政务领域垂直模型、智能体安全内容合规评估和政务领域垂直模型、智能体基础环境脆弱性检测（含资产发现、漏洞检测、配置检测、WEB检测、弱口令检测）等核心能力。

审查政务领域垂直模型及智能体的语料及生成内容风险，发现如提示词注入、不安全的内容输出、模型滥用风险、模型过度依赖、道德伦理风险、违规内容风险和数据泄漏风险等政务领域垂直模型内容安全风险、政务领域垂直模型训练语料风险、政务领域垂直模型基础运行环境（大模型框架、接口等）风险，并对发现的安全风险进行汇总归类，协助下发至相关责任人员，并跟进风险问题至完成复测闭环，对因客观情况无法修复的风险进行标记和记录。

服务要求

内容安全评估：对政务领域垂直模型、智能体的违规内容检测，评估大模型、智能体的抵御恶意输入能力、错误回答率、拒答率等，评估政务领域垂直模型、智能体生成的内容是否准确，是否遵循国家相关法律法规、平台政策、社会规范，避免产生不合规的内容。

基础环境评估：对政务领域垂直模型、智能体的基础运行环境如大模型应用、政务领域垂直模型服务框架等进行扫描评估，包括政务领域垂直模型、智能体的稳定性、鲁棒性、对抗攻击能力等。

语料风险评估：全场景的检测能力，场景覆盖侮辱脏话、身体伤害、歧视偏见、心理健康、违法犯罪、财产隐私、敏感场景、道德伦理等多种，对大模型进行全面、精准的安全检测。

4.5应急演练服务

服务内容

根据应急预案和实际需求，设计详细的应急演练方案，明确演练的目标、内容、场景、参与人员以及演练流程等，场景涵盖可能面临的各类典型突发事件，具有一定的复杂性和挑战性，以充分检验驻场运维团队的应对能力。

按照演练方案组织开展应急演练，模拟真实的突发事件场景，检验应急响应团队在事件预警、应急指挥、协同配合、现场处置等方面的能力。

网络安全事件，选取运维安全监控事件中典型网络安全事件，贴合当前政务系统面临的主流网络安全威胁，采用技术实操+流程推演结合模式，先由技术支撑团队模拟发起对应网络攻击，触发系统安全预警机制，参加演练人员按照应急预案流程，依次完成安全告警排查、攻击源定位、漏洞封堵、全流程操作，同步记录处置时长、操作规范性及问题排查精准度，重点检验团队配合协调流程的适应性。

设备故障事件，选取运维的主干互联网出口和云平台边界作为故障的切入点，模拟链路中断、设备宕机等真实故障场景，技术支撑团队通过工具触发对应故障，引发系统监控告警。参训人员依据应急预案，依次开展故障快速定位（如利用链路诊断工具排查出口链路连通性、分析云平台边界设备运行日志）、应急资源切换（如启用备用互联网链路、激活冗余防火墙节点）、业务恢复验证（确认政务服务对外访问是否恢复正常、云平台对外业务交互是否稳定）等全流程操作，重点检验团队在故障应急响应中的快速决策能力、跨岗位协同效率（如与运营商对接链路修复、与云服务提供商协调设备故障排查）。

对演练效果进行全面评估，分析演练过程中存在的问题和不足之处，提出改进意见和建议，对应急演练进行总结和复盘，将演练过程中的经验教训融入应急响应预案中，进一步完善应急预案。

服务要求

演练场景：每次演练需覆盖不少于3类核心突发场景（网络安全事件，设备故障事件等），全年组织开展规范化应急演练不少于2次。

4.6安全培训服务

服务内容

		定期开展专项安全培训，培训内容需至少包含国家相关网络及数据安全政策/法律法规解读、网络及数据安全风险防范意识，网络及数据安全保护技术解读培训、安全基础常识、安全处置响应、创新安全技术理念等，在培训前需与市数据局确认培训主题，定制符合现场实际需求的培训课程，完成培训课程的相关课件、资料等准备，培训师资视实际培训需求确定，包括但不限于服务方自身提供、聘请外部专家。 人工智能课程培训：提供人工智能课程培训，聚焦人工智能基础安全与通识安全，围绕基础知识、政策标准、安全保障等，为市数据局及相关委办局单位技术、管理岗位人员搭建系统化的AI安全认知体系。 服务要求 服务期内，邀请专家在服务期内完成2次面向西安市数据局关于安全政策、标准、法规解读、人工智能等方面的培训；邀请专家完成2次面向西安市各委办局关于政策、标准、法规解读、人工智能等方面的培训。 4.7人员配置 本项目需配备不少于14名安全运维人员，提供涵盖日常运维、应急响应与处置、重大活动保障、安全监测及安全通告等驻场服务。其中配置项目经理1人，全面统筹项目全周期交付管理，制定计划与目标并协调跨部门资源，推进安全告警闭环；配置技术负责人1人，负责整体安全技术管控，统筹安全核查、应急演练及重大活动保障等专项工作的策划与实施，制定详细方案确保落地；配置运维驻场人员12人，实行区域专属负责制，涵盖政务外网区云外数据中心、安全管理区、互联网行政办公区、政务专网局域网及广域网接入、政务专网数据中心、政务外网园区局域网、云数据中心西咸节点互联网及政务外网边界、互联网业务发布区以及核心交换区等。各驻场人员需实时监测负责区域安全态势，全面排查并上报安全隐患，梳理工作台账，跟踪督办问题整改，并负责各类服务资料的整编与上报，确保各区域安全运维无死角。
--	--	---

采购包2：

标的名称：2026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监理服务

序号	参数性质	技术参数与性能指标
		一、监理服务要求（包括但不限于以下内容） （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。 （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。 （三）服务内容：

1.项目组织及实施方案监理

- (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；
- (2) 审核和确认运维单位的实施人员组织和实施计划安排；
- (3) 审核和确认运维单位的质量保证计划；
- (4) 审核和确认运维单位的进度控制计划。

2.工程组织及总体技术方案的质量控制

- (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。
- (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；
- (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。

3.工程质量控制

- (1) 审核施工单位的运维方案；
- (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；
- (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。；
- (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。
- (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；

4.安全与风险控制

- (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；
- (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；

5.事件进度控制与问题管理

- (1) 建立进度控制协调制度，落实进度控制责任；
- (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；
- (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，避免未经授权的变更。
- (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。
- (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）。
- (4) 协调与承建单位之间的关系，解决纠纷。
- (5) 监督、检查并督促承建单位对用户的培训工作。

13.项目正式验收阶段

- (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。

		(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。 (3) 参加项目正式验收，签署正式验收意见。 (4) 审查承建单位提交的竣工结算申请并报建设单位。 (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。 14.监理服务人员要求 为保障项目监理工作顺利实施，确保项目建设合法合规、规范有序，投标人应组建具有高度政治责任感、丰富从业经验、能够与招标人及承建单位进行良好沟通的高素质团队参与本项目监理工作。 (1) 拟投入本项目的团队人员须为投标单位的正式员工，能够满足本项目监理工作需要，项目团队人员须配备合理，具有不同层次，应至少包括总监理工程师、监理工程师等。 (2) 总监理工程师应承担过类似项目的监理工作，具有信息系统监理师证书。 (3) 总监理工程师不得随意更换，因重大原因确需调整的，须经招标人同意。投标人应根据项目实施阶段工作重点及时调整专业监理人员配置,人员调整必须经招标人同意，招标人有权要求更换人员。 (4) 招标人有权要求投标人保证人员配置的合理性以及团队人员的稳定性，因人员的过失造成招标人的直接经济损失，应赔偿招标人的损失。
--	--	---

3.2.3人员配置要求

采购包1：

本项目需配备不少于14名安全运维人员，提供涵盖日常运维、应急响应与处置、重大活动保障、安全监测及安全通告等驻场服务。其中配置项目经理1人，全面统筹项目全周期交付管理，制定计划与目标并协调跨部门资源，推进安全告警闭环；配置技术负责人1人，负责整体安全技术管控，统筹安全核查、应急演练及重大活动保障等专项工作的策划与实施，制定详细方案确保落地；配置运维驻场人员12人，实行区域专属负责制，涵盖政务外网区云外数据中心、安全管理区、互联网行政办公区、政务专网局域网及广域网接入、政务专网数据中心、政务外网园区局域网、云数据中心西咸节点互联网及政务外网边界、互联网业务发布区以及核心交换区等。各驻场人员需实时监测负责区域安全态势，全面排查并上报安全隐患，梳理工作台账，跟踪督办问题整改，并负责各类服务资料的整编与上报，确保各区域安全运维无死角。

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，专业监理工程师不少于3名，需均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：

满足本项目服务需求的设施设备。

采购包2：

满足本项目服务需求的设施设备。

3.2.5其他要求

采购包1：

质量要求：合格（达到国家强制性合格标准）及招标人对本项目的服务要求。

采购包2：

质量要求：合格（达到国家强制性合格标准）及招标人对本项目的服务要求。

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:

招标人指定地点

采购包2:

招标人指定地点

3.3.3考核（验收）标准和方法

采购包1:

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:

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:

- 1、进度款，合同签订后，达到付款条件起30个工作日内，支付合同总金额的30.0%
- 2、进度款，服务满6个月，经阶段验收合格，达到付款条件起30个工作日内，支付合同总金额的40.0%
- 3、进度款，服务期满，经验收合格，达到付款条件起30个工作日内，支付合同总金额的30.0%

采购包2:

- 1、进度款，合同签订后，达到付款条件起10个工作日内，支付合同总金额的30.0%
- 2、进度款，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个工作日内，支付合同总金额的40.0%
- 3、进度款，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个工作日内，支付合同总金额的30.0%

3.3.6违约责任与解决争议的方法

采购包1:

详见合同约定

采购包2:

详见合同约定

3.4其他要求

质量要求：合格（达到国家强制性合格标准）及招标人对本项目的服务要求。

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；	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

采购包2：

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；	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	供应商为向招标人提供相关服务的法人或其他组织；	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 投标人应提交的相关资格证明材料
2	信用要求	供应商未被“信用中国”网站列入“重大税收违法失信主体名单”；未被“中国执行信息公开网”列入“失信被执行人”；未被“中国政府采购网”网站列入“政府采购严重违法失信行为记录名单”；未被“国家企业信用信息公示系统”网站“列入严重违法失信名单（黑名单）信息”；	附件12授权书.docx 中小企业声明函 残疾人福利性单位声明函 附件11--承诺书.docx 监狱企业的证明文件 投标人应提交的相关资格证明材料
3	财务报告	供应商提供2025年度经审计完整的财务审计报告（成立时间至提交响应文件截止时间不足一年的可提供自成立以来的资产负债表）或在开标日期前六个月内其基本开户银行出具的资信证明。	投标人应提交的相关资格证明材料
4	社保的缴费证明材料	提供递交响应文件截止时间前一年内至少一个月已缴纳的社会保障资金的凭据（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供应商应提供相关文件证明；	投标人应提交的相关资格证明材料
5	纳税的缴费证明材料	供应商递交响应文件截止时间前一年内至少一个月依法缴纳税收的相关凭据（时间以税款所属日期为准，税种须包含增值税或企业所得税，凭据应有税务机关或代收机关的公章或业务专用章）；其他组织和自然人提供缴纳税收的凭据；依法免征、零申报的供应商应提供相关文件证明材料。	投标人应提交的相关资格证明材料

采购包2：

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	供应商为向招标人提供相关服务的法人或其他组织；	附件12授权书.docx 中小企业声明函 残疾人福利性单位声明函 附件11--承诺书.docx 监狱企业的证明文件 投标人应提交的相关资格证明材料
2	信用要求	供应商未被“信用中国”网站列入“重大税收违法失信主体名单”；未被“中国执行信息公开网”列入“失信被执行人”；未被“中国政府采购网”网站列入“政府采购严重违法失信行为记录名单”；未被“国家企业信用信息公示系统”网站“列入严重违法失信名单（黑名单）信息”；	附件12授权书.docx 中小企业声明函 残疾人福利性单位声明函 附件11--承诺书.docx 监狱企业的证明文件 投标人应提交的相关资格证明材料
3	财务报告	供应商提供2025年度经审计完整的财务审计报告（成立时间至提交响应文件截止时间不足一年的可提供自成立以来的资产负债表）或在开标日期前六个月内其基本开户银行出具的资信证明。	投标人应提交的相关资格证明材料
4	社保的缴费证明材料	提供递交响应文件截止时间前一年内至少一个月已缴纳的社会保障资金的凭据（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供应商应提供相关文件证明；	投标人应提交的相关资格证明材料
5	纳税的缴费证明材料	供应商递交响应文件截止时间前一年内至少一个月依法缴纳税收的相关凭据（时间以税款所属日期为准，税种须包含增值税或企业所得税，凭据应有税务机关或代收机关的公章或业务专用章）；其他组织和自然人提供缴纳税收的凭据；依法免征、零申报的供应商应提供相关文件证明材料。	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			

采购包2：

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	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。	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 附件12授权书.docx 中小企业声明函 商务应答表 附件11--承诺书.docx 服务内容及服务要求 应答表 附件14租赁设备.docx 投标人应提交的相关资格证明材料 投标函 附件15-其他.docx 残疾人福利性单位声明函 服务方案 标的清单 投标文件封面 附件10-业绩表.docx 监狱企业的证明文件

采购包2：

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 附件12授权委托书.docx 中小企业声明函 商务应答表 附件11--承诺书.docx 服务内容及服务要求 应答表 投标人应提交的相关资格证明材料 投标函 附件15-其他.docx 残疾人福利性单位声明函 服务方案 标的清单 投标文件封面 附件10-业绩表.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。

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：

评审内容		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
	企业业绩	投标人应在投标文件中提供该投标人近三年（2023年1月1日）至今的类似业绩证明材料，每提供一份有效类似业绩证明材料的得2分，满分10分。注：需提供合同证明材料，包括但不限于合同首页、签字盖章页、内容页，以上材料缺少任意一项视为未提供。上述内容需提供证明材料复印件并加盖公章。提供材料不清晰、缺项或无法辨认的视为未提供，不计分。	10.0000	客观	服务方案 附件10-业绩表.docx

团队人员	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经理具有信息系统项目管理师证书，得3分； 2.拟担任本项目的技术负责人具有注册信息安全专业人员（CISP）证书，得3分； 3.运维团队（不包括项目经理及技术负责人）：供应商为本项目配备不少于12人驻场运维团队（少于12人不得分），供应商拟派团队人员（满分8分）： ①至少1人具备信息系统项目管理师证书，得1分； ②至少1人具备信息安全工程师证书，得1分； ③至少1人具备注册信息安全专业人员（CISP）证书，得1分； ④至少1人具备数据安全工程师证书，得1分； 备注：需提供合法有效的证书扫描件；项目经理、技术负责人不可为同一人；单人具有多个证书不重复计分，本项最高计14分。	14.0000	客观	商务应答表 服务方案
企业实力	1.管理体系认证（5分） 投标人具备ISO9001质量管理体系认证证书或ISO27001信息安全管理体或ISO20000信息技术服务管理体系认证证书或ISO/IEC 27017云服务信息安全管理体证书或 ISO45001职业健康安全管理体系中的任意一项的得1分，满分5分。	5.0000	客观	商务应答表 服务方案
项目分析	根据投标人对项目整体及重点难点的分析赋分。 1.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； 2.提供了相关分析，但内容简单，无应对策略，得3分； 3.相关分析或与实际不符，得1分； 4.未提供项目分析，得0分。	5.0000	主观	商务应答表 服务方案

详细评审	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	商务应答表 服务方案 服务内容及服务要求 应答表
	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.技术参数全部满足项目需求，得16分；2.技术参数负偏离未超过10项，得8分；3.技术参数负偏离超过10项（含10项），得0分。	16.0000	客观	商务应答表 服务方案
	总体服务方案	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；②终端准入认证服务；③统一安全运维服务；④安全检测服务等方面赋分：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4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.服务方案偏差较大，整体框架存在较大缺陷，服务内容阐述较为模糊的，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4分，共16分。	16.0000	主观	服务方案

质量保障方案	投标人提供的质量保障方案的思路及要点需包含①质量目标；②质量保障方法及措施，共2项内容，每项满分3分，总分6分。单项方案切实可行，能够完全保障项目顺利实施的，得3分； 单项方案内容较为完善，能够有效保障项目顺利实施的，得2分； 单项方案内容粗糙，不能有效保障项目顺利实施的，得1分； 单项方案内容严重缺失或者未提供相应方案的，得0分；	6.0000	主观	商务应答表 服务方案
风险管理方案	投标人提供的风险管理方案的思路及要点需包含①风险管控方案；②应急响应预案，共2项内容，每项满分1.5分，总分3分。单项方案切实可行，能够完全保障项目顺利实施的，得1.5分； 单项方案内容较为完善，能够有效保障项目顺利实施的，得1分； 单项方案内容粗糙，不能有效保障项目顺利实施的，得0.5分； 单项方案内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案

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50%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×50%。（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50%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×50%。（3）投标（响应）报价低于最高限价45%的，即投标（响应）报价<最高限价×45%。（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	投标函 开标一览表 标的清单
价格分	价格分	经初审合格的投标文件，其投标报价为有效投标价。评审基准价：即满足招标文件要求且投标报价最低的为评审基准价。其他投标人的价格分统一按照下列公式计算。 价格分=（评审基准价/投标报价）×10	10.0000	客观	开标一览表 标的清单

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
无					

采购包2：

评审内容		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
	企业业绩	供应商应在投标文件中提供该供应商自2023年1月1日起至至今的类似业绩证明材料，每提供一份有效类似业绩证明材料的得3分，满分12分。注：需提供合同证明材料，包括但不限于合同首页、签字盖章页、内容页，以上材料缺少任意一项视为未提供。上述内容需提供证明材料复印件并加盖公章。提供材料不清晰、缺项或无法辨认的视为未提供，不计分。	12.0000	客观	商务应答表 服务方案
	服务要求的响应	根据供应商针对服务要求响应情况进行评审，完全响应并满足服务要求的得25分，有一项未响应或不满足采购需求的扣0.5分，扣完为止，总分25分。备注：相应的各服务要求均需提供佐证材料。佐证材料为供应商认为可以佐证参数响应性的材料。供应商对材料的真实性、完整性、有效性及针对性承担责任，自行承担因材料提供不全导致服务要求被认定为不满足或负偏离的风险。	25.0000	客观	商务应答表 服务方案

监理实施方案	根据投标人提供的针对本项目制定的监理实施方案，包括①监理总体的工作目标②监理内容③服务方式④监理流程等方面进行评审，共4项内容，每项满分1.5分，总分6分。单项方案切实可行，能够完全保障项目顺利实施的，得1.5分；单项方案内容较为完善，能够有效保障项目顺利实施的，得1分；单项方案内容粗糙，不能有效保障项目顺利实施的，得0.5分；单项方案内容严重缺失或者未提供相应方案的，得0分。	6.0000	主观	商务应答表 服务方案
质量控制管理措施	根据投标人提供的针对本项目制定的质量控制管理措施方案，包括①核心环节质量管控措施；②整改机制及完善的售后服务体系，共2项内容，每项满分1.5分，总分3分。单项措施切实可行，能够完全保障项目顺利实施的，得1.5分；单项措施内容较为完善，能够有效保障项目顺利实施的，得1分；单项措施内容粗糙，不能有效保障项目顺利实施的，得0.5分；单项措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案
进度控制管理措施	根据投标人提供的针对本项目制定的进度管理及管控措施方案，包括①进度计划及时间节点；②工作内容，每项满分1.5分，总分3分。单项措施切实可行，能够完全保障项目顺利实施的，得1.5分；单项措施内容较为完善，能够有效保障项目顺利实施的，得1分；单项措施内容粗糙，不能有效保障项目顺利实施的，得0.5分；单项措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案

变更控制的方法和措施	根据投标人提供的针对本项目制定的变更控制的方法和措施，包括对①变更控制方法、变更控制措施，共1项内容，每项满分3分，总分3分。措施切实可行，能够完全保障项目顺利实施的，得3分；措施内容较为完善，能够有效保障项目顺利实施的，得2分；措施内容粗糙，不能有效保障项目顺利实施的，得1分；措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案
投资控制的方法和措施	根据投标人提供的针对本项目制定的项目投资控制方案，包括对项目投资的控制方法及措施，共1项内容，每项满分3分，总分3分。投资控制的方法和措施切实可行，能够完全保障项目顺利实施的，得3分；投资控制的方法和措施内容较为完善，能够有效保障项目顺利实施的，得2分；投资控制的方法和措施内容粗糙，不能有效保障项目顺利实施的，得1分；投资控制的方法和措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案

详细评审	信息安全控制措施	根据投标人提供的针对本项目制定的满足项目要求和信息安全标准的信息安全控制措施方案，包括①信息安全控制措施、项目信息安全控制措施，共1项内容，每项满分3分，总分3分。信息安全控制措施、项目信息安全控制措施切实可行，能够完全保障项目顺利实施的，得3分；信息安全控制措施、项目信息安全控制措施内容较为完善，能够有效保障项目顺利实施的，得2分；信息安全控制措施、项目信息安全控制措施内容粗糙，不能有效保障项目顺利实施的，得1分；信息安全控制措施、项目信息安全控制措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案
	合同和文档管理的措施	根据投标人提供的针对本项目制定的满足项目安全运维服务监理和项目审计的合同和文档管理方案，包括合同文档管理措施及合同文档管理制度，共1项内容，每项满分3分，总分3分。合同和文档管理的措施切实可行，能够完全保障项目顺利实施的，得3分；措施内容较为完善，能够有效保障项目顺利实施的，得2分；措施内容粗糙，不能有效保障项目顺利实施的，得1分；措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案

组织协调的方法和措施	根据投标人提供的针对本项目制定的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的组织协调方案，包括①组织协调的协调范围与对象②组织协调的风险评估与应对，共2项内容，每项满分1.5分，总分3分。措施切实可行，能够完全保障项目顺利实施的，得1.5分；措施内容较为完善，能够有效保障项目顺利实施的，得1分；措施内容粗糙，不能有效保障项目顺利实施的，得0.5分；措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 服务方案
保密措施	根据投标人提供的针对本项目制定的保密方案，包括①安全保密职责②安全保密措施，共2项内容，每项满分1.5分，总分3分。措施切实可行，能够完全保障项目顺利实施的，得1.5分；措施内容较为完善，能够有效保障项目顺利实施的，得1分；措施内容粗糙，不能有效保障项目顺利实施的，得0.5分；措施内容严重缺失或者未提供相应方案的，得0分。	3.0000	主观	商务应答表 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，共1项内容，每项满分3分，总分3分。建议或意见切实可行，能够完全保障项目顺利实施的，得3分；建议内容较为充足，能够有效保障项目顺利实施的，得2分；建议内容粗糙，不能有效促进项目实施的，得1分；建议的内容严重缺失或者未提供相应建议的，得0分。	3.0000	主观	商务应答表 服务方案

企业资质信	投标人具有①ISO 27001信息安全管理体系认证证书；②ISO 20000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	商务应答表 服务方案
监理团队	项目监理团队配备项目总监理工程师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），同时提供截至投标文件递交截止时间前供应商为其缴纳的近六个月任意一个月的社保缴纳证明扫描件，未按上述要求提供相关证明材料的，本项不得分。在满足上述要求基础上，根据以下要求进行评审： 1.总监理工程师（9分）（1）供应商拟派的总监理工程师具备信息系统项目管理师证书或信息系统监理工程师资质证书任意一项证书的得2分，满分4分。 （2）近三年（2023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5分。企业业绩和拟派总监理工程师业绩可重复计分。备注：以供应商提供的合同复印件或扫描件为准，需体现项目总监理工程师姓名，时间以合同中所体现的时间为准。 2.专业监理工程师（3分） 供应商拟派的专业监理工程师每有一人具备信息系统项目管理师证书的得1分，满分3分。	12.0000	客观	商务应答表 服务方案

团队架构	供应商提供的服务团队配备情况需包含①人员配置情况表；②各流程节点岗位职责划分及岗位管理机制，共2项内容，每项满分3分，总分6分。其中：人员配备方案（3分）人员充足，经验丰富，证书齐全有效，能够完全胜任本项目服务需求的，得3分；人员较为充足，有一定的经验，多数人员能持证上岗的，得2分；人员配备较为欠缺，无后备力量支撑，缺乏机动性，得1分；人员配备不能够满足本项目服务需求的，或者所有人员都不能持证上岗的，得0分；各流程节点岗位职责划分及岗位管理机制（3分）各流程节点岗位职责划分明确、岗位管理机制合理，得3分；各流程节点岗位职责划分较为明确、岗位管理机制存在部分不利于项目实施的，得2分；各流程节点岗位职责划分混乱、岗位管理机制不科学的，得1分；各流程节点岗位职责划分及岗位管理机制存在重大缺陷或者未提供的，得0分；	6.0000	客观	商务应答表 服务方案
------	--	--------	----	---------------

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50%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×50%。（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50%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×50%。（3）投标（响应）报价低于最高限价45%的，即投标（响应）报价<最高限价×45%。（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	投标函 开标一览表 标的清单
价格分	价格分	经初审合格的投标文件，其投标报价为有效投标价。评审基准价：即满足招标文件要求且投标报价最低的为评审基准价。其他投标人的价格分统一按照下列公式计算。 价格分=（评审基准价/投标报价）×10	10.0000	客观	开标一览表 标的清单

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
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：服务内容及服务要求应答表
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：服务方案
详见附件：附件14租赁设备.docx
详见附件：附件10-业绩表.docx
详见附件：附件11--承诺书.docx
详见附件：附件12授权书.docx
详见附件：附件15-其他.docx

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：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：服务内容及服务要求应答表
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：服务方案
详见附件：附件10-业绩表.docx
详见附件：附件11--承诺书.docx
详见附件：附件12授权书.docx
详见附件：附件15-其他.docx

第七章 拟签订采购合同文本

详见附件：公开招标文件模板.docx