

招 标 文 件

(服务类)

采购项目名称：陕西省数字政府网络安全监测提升及服务优化项目

采购项目编号：HCXM-GK-2501-08

陕西省政务大数据服务中心

汇成项目管理有限公司共同编制

2025年02月07日

第一章 投标邀请

汇成项目管理有限公司（以下简称“代理机构”）受陕西省政务大数据服务中心委托，拟对陕西省数字政府网络安全监测提升及服务优化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：HCXM-GK-2501-08

二、采购项目名称：陕西省数字政府网络安全监测提升及服务优化项目

三、招标项目简介

陕西省数字政府网络安全监测提升及服务优化项目是贯彻落实《陕西省数字政府建设“十四五”规划》三大运行保障要求和“五位一体”安全要求，对标外省先进做法，实现大安全目标，持续提升数字政府安全感知、风险管理能力。采购内容：采购包1：网络安全管理监督服务；采购包2：网络安全管理运营服务。（具体内容详见招标文件）

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：

无

（三）本项目的特定资格要求：

采购包1：

1、本项目的特定资格要求：1、有效的主体资格证明：投标供应商为具有独立承担民事责任能力的法人或其他组织。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件；2、法定代表人授权书/身份证明书：法定代表人直接参与投标的，须递交《法定代表人身份证明书》和身份证复印件。法定代表人授权代表参加投标的，须递交《法定代表人授权委托书》及授权代表身份证复印件；3、财务状况：提供具有财务审计资质单位出具的完整2023年度的财务报告（成立时间至投标文件递交截止时间不足一年的可提供成立后任意时段的资产负债表）或投标文件递交截止时间前六个月内其开户银行出具的资信证明；4、社会保障资金缴纳证明：供应商提供2024年至今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供应商应提供相关文件证明；5、税收缴纳证明：供应商提供2024年度至今至少一个月的纳税证明或完税证明，纳税证明或完税证明上应有代收机构或税务机关的公章，依法免税的供应商应提供相关文件证明；6、专业技术能力的声明：提供具有履行本合同所必需的专业技术能力的声明。7、无重大违法记录声明：供应商应具备良好的商业信誉，提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明；8、信用记录查询结果：供应商应在投标截止日前，以“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）国家企业信用信息公示系统

（<https://www.gsxt.gov.cn/index.html>）截图查询结果为准，提供（查询日期为从招标文件发售之日起至投标截止日前）网站截图并加盖供应商公章（开标当天代理机构现场查询，若不符合要求，按无效标处理），查询内容为未被列入失信被执行人、重大税收违法案件当事人名单（处罚期限届满的除外）和政府采购严重违法失信行为记录。9、企业关联关系声明：单位负责人为同一人或者存在直接控股、管理关系的不同投标供应商，不得参加同一合同项下的政府采购活动；注：本项目不接受联合体投标。

采购包2：

1、本项目的特定资格要求：1、有效的主体资格证明：投标供应商为具有独立承担民事责任能力的法人或其他组织。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件；2、法定代表人授权书/身份证明书：法定代表人直接参与投标的，须递交《法定代表人身份证明书》和身份证复

印件。法定代表人授权代表参加投标的，须递交《法定代表人授权委托书》及授权代表身份证复印件； 3、财务状况：提供具有财务审计资质单位出具的完整**2023**年度的财务报告（成立时间至投标文件递交截止时间不足一年的可提供成立后任意时段的资产负债表）或投标文件递交截止时间前六个月内其开户银行出具的资信证明； 4、社会保障资金缴纳证明：供应商提供**2024**年至今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供应商应提供相关文件证明； 5、税收缴纳证明：供应商提供**2024**年度至今至少一个月的纳税证明或完税证明，纳税证明或完税证明上应有代收机构或税务机关的公章，依法免税的供应商应提供相关文件证明； 6、专业技术能力的声明：提供具有履行本合同所必需的专业技术能力的声明。 7、无重大违法记录声明：供应商应具备良好的商业信誉，提供参加政府采购活动前**3**年内在经营活动中没有重大违法记录的书面声明； 8、信用记录查询结果：供应商应在投标截止日前，以“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）国家企业信用信息公示系统

（<https://www.gsxt.gov.cn/index.html>）截图查询结果为准，提供（查询日期为从招标文件发售之日起至投标截止日前）网站截图并加盖供应商公章（开标当天代理机构现场查询，若不符合要求，按无效标处理），查询内容为未被列入失信被执行人、重大税收违法案件当事人名单（处罚 期限届满的除外）和政府采购严重违法失信行为记录。 9、企业关联关系声明：单位负责人为同一人或者存在直接控股、管理关系的不同投标供应商，不得参加同一合同项下的政府采购活动； 注：本项目不接受联合体投标。

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：陕西省政务大数据服务中心

地址：西安市新城区新城大院

邮编：710000

联系人：陕西省数据和政务服务中心经办

联系电话：029-63912526

代理机构：汇成项目管理有限公司

地址：陕西省西安市雁塔区团结南路12西安国际人才大厦A座北1508

邮编：710075

联系人：刘婧莎

联系电话：029-68781555

采购监督机构：财政厅政府采购管理处

联系人：柴老师、杨老师

联系电话：029-68936409、029-68936410

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1：702,500.00元</p> <p>采购包2：16,294,700.00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。</p> <p>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。</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 | <p>采购包1保证金金额：10,000.00元</p> <p>采购包2保证金金额：100,000.00元</p> <p>缴交渠道：电子保函,转账、支票、汇票等（需通过实体账户、户名及开户行信息）</p> <p>开户名称：汇成项目管理有限公司（备注：缴纳时需备注项目名称、采购包号；开具保函的单位，在投标截止前一天需给代理机构交一份纸质版保函。）</p> <p>开户银行：中国建设银行股份有限公司西安高新科技支行</p> <p>银行账号：61050192570000000294</p> |
| 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：缴纳</p> <p>本采购包履约保证金为合同金额的5.0%</p> <p>说明：说明：缴纳中标金额的5%（服务期结束后退还，扣除标准依据双方合同约定）</p> <p>采购包2：缴纳</p> <p>本采购包履约保证金为合同金额的5.0%</p> <p>说明：说明：缴纳中标金额的5%（服务期结束后退还，扣除标准依据双方合同约定）</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：采购人</p> <p>代理服务费收费标准：参照原《国家计委关于印发<招标代理服务收费管理暂行办法>的通知》（计价格〔2002〕1980号）、《国家发展改革委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〔2015〕299号）规定执行。服务费账户信息：户名：汇成项目管理有限公司账号：6105 0192 5700 0000 0294开户行：中国建设银行股份有限公司西安高新科技支行</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 | <p>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；</p> <p>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。</p> |
| 17 | 进口产品 | 不允许 |
| 18 | 是否组织潜在投标人现场考察 | <p>采购包1：组织现场踏勘：否</p> <p>采购包2：组织现场踏勘：否</p> |
| 19 | 特殊情况 | <p>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：</p> <p>（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；</p> <p>（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；</p> <p>（三）其他无法保证电子化交易的公平、公正和安全的情况。</p> <p>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。</p> <p>（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；</p> <p>（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；</p> <p>（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。</p> |

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陕西省政务大数据服务中心和汇成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，评标细则及标准由陕西省政务大数据服务中心负责解释。除上述招标文件内容，其他内容由汇成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陕西省政务大数据服务中心。

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

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是汇成项目管理有限公司。

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、推荐中标候选人等活动。

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：

依招标文件和最终签订合同为准

采购包2：

依招标文件和最终签订合同为准

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 汇成项目管理有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由汇成项目管理有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 汇成项目管理有限公司 负责答复。

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

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

四、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：（一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日；（二）对采购过程提出质疑的，为各采购程序环节结束之日；（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

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

六、供应商提出质疑时应当准备的资料

（一）质疑函正本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：刘婧莎

联系电话：**029-68781555**

地址：陕西省西安市雁塔区团结南路西安国际人才大厦**A座北1508**

邮编：**710075**

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

陕西省数字政府网络安全监测提升及服务优化项目是贯彻落实《陕西省数字政府建设“十四五”规划》三大运行保障要求和“五位一体”安全要求，对标外省先进做法，实现大安全目标，持续提升数字政府安全感知、风险管理能力。采购内容：采购包1：网络安全管理监督服务；采购包2：网络安全管理运营服务。（具体内容详见招标文件）

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）：702,500.00
采购包最高限价（元）：702,500.00
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 | 网络安全管理 监督服务 | 1. 0 0 | 702,500. 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）：16,294,700.00
采购包最高限价（元）：16,294,700.00
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 | 网络安全管理 运营服务 | 1. 0 0 | 16,294,7 00.00 | 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：
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
标的名称：网络安全管理监督服务

| 参数性质 | 序号 | 技术要求名称 | 技术参数与性能指标 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------|--------------|--------|--|------|------------|--------|----------|----------|------------|----|------|----|--------------|------|------|--------|----------|----------|------------|---|------------|---|-------|---|------------|---|---|---|---|----|------|----|----|----|---|--------------|---|---|--|
| | | | <div>采购内容及要求</div> <div><p>（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。）</p><p>一、采购项目名称</p><p>陕西省数字政府网络安全监测提升及服务优化项目</p><p>二、采购项目概况</p><p>陕西省数字政府网络安全监测提升及服务优化项目是贯彻落实《陕西省数字政府建设“十四五”规划》三大运行保障要求和“五位一体”安全要求，对标外省先进做法，实现大安全目标，持续提升数字政府安全感知、风险管理能力。本项目包含采购包1：网络安全管理监督服务、采购包2：网络安全管理运营服务。</p><p>三、采购包1采购需求</p><p>1、服务内容</p><p>采购包预算金额（万元）：70.25</p><p>采购包最高限价（万元）：70.25</p><p>供应商报价不允许超过标的金额</p><p>（招单价的）供应商报价不允许超过标的单价</p><table><tr><th>序号</th><th>标的名称</th><th>数量</th><th>标的金额 (万元)</th><th>计量单位</th><th>所属行业</th><th>是否核心产品</th><th>是否允许进口产品</th><th>是否属于节能产品</th><th>是否属于环境标志产品</th></tr><tr><td>1</td><td>网络安全管理监督服务</td><td>1</td><td>70.25</td><td>项</td><td>软件和信息技术服务业</td><td>否</td><td>否</td><td>否</td><td>否</td></tr></table><p>采购服务内容清单</p><table><tr><th>序号</th><th>服务名称</th><th>数量</th><th>单位</th><th>备注</th></tr><tr><td>1</td><td>网络安全管理监督规范服务</td><td>1</td><td>项</td><td></td></tr></table></div> | | | | | | | 序号 | 标的名称 | 数量 | 标的金额 (万元) | 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 | 网络安全管理监督服务 | 1 | 70.25 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 | 序号 | 服务名称 | 数量 | 单位 | 备注 | 1 | 网络安全管理监督规范服务 | 1 | 项 | |
| 序号 | 标的名称 | 数量 | 标的金额 (万元) | 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 | 网络安全管理监督服务 | 1 | 70.25 | 项 | 软件和信息技术服务业 | 否 | 否 | 否 | 否 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 序号 | 服务名称 | 数量 | 单位 | 备注 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 网络安全管理监督规范服务 | 1 | 项 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | |
|---|----------------|---|---|--|
| 2 | 网络安全管理评价规范服务 | 1 | 项 | |
| 3 | 网络安全管理运营评价服务 | 1 | 项 | |
| 4 | 安全管理技术运营合规审计服务 | 1 | 项 | |

1.1服务要求

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

标的名称：网络安全管理监督服务

1.2服务目标

落实《陕西省数字政府建设“十四五”规划》中关于网络安全的有关要求。根据当前需求、解读国家相关法律法规、标准规范，并对网络安全管理责任范围内的各项工作内容发布评价规范指标；针对作为网络安全管理抓手的网络安全管理运营制定详细的评价指标促进发挥其作用；针对网络安全管理运营服务方的服务工作、服务成果、服务质量等进行综合评价和合规审计；通过以上目标的落实，便于局和中心在整体规范、责权清晰、技管互补、多方协同、管理务实、监督得当的环境下更好的开展各项工作。

1.3网络安全管理监督规范服务

协助局和中心完成年度省数字政府网络和数据安全管理标准规范、管理监督总结报告，发布安全风险评估管理标准规范、日常安全检查管理流程、人力资源安全管理标准规范，管理指标及考核管理标准规范、管理监管接口及数据标准管理标准规范；各项规范应能配合完成网络安全管理运营服务的整体监督。完成周报、月报、服务期内总结报告、网络安全管理监督规范服务标准、监督分析报告等。

1.4网络安全管理评价规范服务

协助局和中心完成省数字政府管理评价，制定网络安全管理总体设计、网络安全管理技术规范、网络安全监督规范详细的评价指标，发布源代码审计服务规范、渗透测试服务规范、网络安全评估规范、攻防演练规范、供应链安全风险评估规范等管理标准规范；制定各项内容的评价标准共完成评价报告。完成周报、月报、服务器内总结报告、网络安全管理评价规范服务标准等。

1.5安全管理运营评价服务

协助局和中心完成网络安全管理运营服务方评价报告，完成工作绩效指标、工作进展、工作过程、输出物考核，度量和考核服务方各项服务的完成度、完成绩效、完成质量优略等具体技术工作。辅助数字政府管理单位完成对网络安全管理运营服务方的考核，用于运营服务计费。调研现有运营方式，制定必要的评价指标和评价方法，规划评价操作方式，并按照实际验证的评价指标和方法，完成技术评价的平台化规划设计。完成周报、月报、服务周期总结报告、网络安全管理运营服务评价规范、安全管理运营评价报告。

1.6安全管理技术运营合规审计服务

协助局和中心完成对网络安全管理运营服务方的服务人员、服务工具、服务流程、服务过程、服务成果等的综合性合规审计，确保网络安全管理运营服务方提供的服务自身不引入新的安全风险，其运营过程不带入新的安全风险，其运营结果不造成新的安全风险。完成周报、月报、总结报告、网络安全管理运营审计过程总结报告、运营审计整改建议报告、运营合规审计报告、运营服务合规审计规范。

2、人员配置要求

▲服务人员要求。服务团队成员不少于8人；团队负责人1人，5年以上相关工作经验，具备高级工程师（信息化类）、信息系统项目管理师、咨询工程师证书；网络安全专业人员1人，10年以上网络安全相关工作经验，具备CISP证书(注册信息安全专业人员)、CCSC证书（网络与信息安全应急人员），网络安全高级工程师职业资格（工信认证）；项目专家人员2人，10年以上信息化咨询经验，具备人社评定的高级工程师（信息化类）；项目组成员4人，3年以上工作经验，具备咨询工程师证书。提供网络安全专业人员1人、专家人员2人，共3人的驻场工作，且实际服务



1

采购内容及要求

人员不变更的承诺函。中标人须书面承诺，如在项目执行过程中服务团队不能胜任相关工作的，采购人有权要求更换，中标人自收到采购人的人员更换要求之日起两周内安排符合采购文件要求且能胜任相关工作的人员到场。如须调整服务团队成员，中标人须书面向采购人提出申请并取得采购人同意后调整。以上要求如有违反，则视为违约行为，采购人有权终止服务合同。

3、设施设备配置要求

投标人按照服务响应时间需求、人员需求自行准备本地化服务所需的设施。

▲投标人自行提供评价管理平台，平台系统满足云化和国产化部署要求，具备服务所需数据的接入能力、交付成果管理能力、管理过程数据展示能力等，并可按照采购人要求自定义指标库管理，指标库涵盖信息安全风险管理所需各类指标项内容，提供标准化指标项并可自定义管理指标项内容，通过指标选取、测量周期配置、指标值分制设置等，可自动计算指标得分；对于风险管理目标可实现同步性指标管理；提供运营分析能力，基于综合运营、质量分析、合规分析、人员分析、能力分析、自定分析得出安全管理指标数据；有效反应并管理网络安全运营服务、网络安全监督服务的服务进度及服务质量；服务开始时平台需直接投入适用，提供证明材料。采购人享有工具使用权和工具使用过程中产生的数据的所有权，未经采购人允许不得随意停止、撤换平台化工具。

在采购人现场工作的投标人驻场服务人员，现场服务时需随身佩戴工作证件，标明岗位、负责事务，遵守局和中心的规章制度及工作守则，办公期间不从事与现场岗位无关的活动。服务人员未征得同意，不得使用相关用户的计算机，不得随意翻看用户办公资料物品；未经同意，不得拍摄、传播、留存用户相关数据信息；服务人员不得越权使用云网基础设施、系统、平台等的任何功能；不得私自拷贝用户业务系统中的任何数据和程序；所有重要操作行为均需进行报备方可进行，并对操作行为和结果进行记录。

项目服务期间应保障采购人现有网络系统、应用系统的正常运行，未经采购人允许不得擅自改动网络系统现状、业务系统配置，包括但不限于：网络架构和设备端口关系、设备IP配置、策略配置、系统参数、应用系统参数等。

4、管理要求

▲总体交付标准应符合政策性文件、国标及需求标准，并对交付内容给出实质性可落地的规划方案，交付文档要求应符合档案管理内容；整体过程管理要中应符合服务相关要求；具备必要的资质和能力；整体交付过程中应满足信息安全风险管理要求，具备信息安全风险评估能力，按照政策性、标准性、事件性等变化趋势动态评估各项内容的管理风险完成对应规范、标准的及时修订更新；配置有专家库资源，随时支撑重大风险会商、专家响应咨询；整个过程数据应自带平台化工具完成各项工作的动态实时管理指标分析和展示，便于采购方实时掌握安全管理的风险状态。针对总体要求给出详细的方案内容。

5、质量要求

投标人应严格按照质量体系的规定，制定项目质量控制措施，保证在项目执行的各个阶段均得到有效控制，所有质量控制过程均应有质量记录，以便进行服务全流程质量的追溯。

对于合同的各个阶段，投标人必须制订和执行质量保证监督计划，清楚地阐明对各个阶段的检查验收和测试方法，确保项目实施的各项内容都能满足国家标准和采购单位要求。

（1）项目全过程监理

本项目引入监理制，监理对本项目进行全过程的监督。投标人在项目组织和实施计划中应考虑到监理要求，实施过程中要积极配合监理工作，以保证项目实施的进度和质量。

（2）项目全过程监督

本项目由采购人对本项目网络安全管理监督服务单位进行全过程的监督，监督、评价、审计，评价结果影响服务方的最终服务费用。投标人在项目组织和实施计划中应考虑到监督要求，实施过程中要积极配合监督工作，以保证项目服务的质量。按照采购人制定的考核标准进行考核，考核结果应用于费用结算。

（3）文档管理

在项目实施过程中，由于项目实施的复杂性，双方人员参加以及时间跨度长等因素，所以有关过程文档都需文档

化、标准化，以便查阅和引用。实施文档应作为项目成果的组成部分。

项目文档至少应包括：项目管理文档、服务过程文档、服务团队提交并由客户确认的相关文档、服务成果文档、客户签署的阶段成果确认书、项目总结报告等。

文档管理内容主要包括文档命名标准、文档的版本控制、文档的批准和存档，最终交付文档需满足档案管理要求。

6、交付标准

投标人必须具备检验机构认可资质、信息安全风险评估资质、信息安全应急处理服务资质等专业能力资质，具有相关服务经验和本地化服务能力。服务人员完成服务的交付，人员具备本项目要求相关的资历，资质证书需为国家权威机构颁发的证书，非行业协会证书。

本项目所有服务成果交付需满足服务要求中各项服务的服务成果及交付标准，服务过程及执行技术标准满足网络安全管理监督服务单位制定的服务技术标准规范和考核评价要求，所有服务成果资料通过评价管理平台完成在线管理和流转。

招标需求中的要求均为最低需求，投标人需根据实际服务需求，考虑增量和突发情况，根据实际完成全部服务要求，服务期内不增加任何费用。

7、验收标准

项目验收按照省级项目验收的有关规定执行。项目验收的具体组织工作由项目采购人承担。同时应完成下列内容：

- 1) 合同、招标文件、投标文件明确的服务内容。
- 2) 项目验收包括按照合同和根据招标文件所编写的投标文件中相关的全部文档。
- 3) 平台化工具的相关留存数据、分析结果数据。

8、成果归属

1.中标人为履行本项目义务所形成的服务成果的知识产权归采购人所有。本项目不会引起任何已申请、登记的知识产权所有权的转移。

2.本合同所涉及的数据所有权归政府所有。中标人只能用于履行本合同之义务。

3.中标人提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权等方面的有关规定和要求。

▲4.中标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因中标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，中标人应负责解决并赔偿因此给采购人造成的全部损失。

9、保密要求

▲中标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。中标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。中标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人内部与该项目无关的任何人员。

10、商务要求

(1) 采购服务期限：七个月

(2) 验收标准

项目验收按照省级项目验收的有关规定执行。项目验收的具体组织工作由项目采购人承担。同时应完成下列内容：

- 1) 合同、招标文件、投标文件明确的服务内容。

| | | |
|--|--|--|
| | | <p>2) 项目验收包括按照合同和根据招标文件所编写的投标文件中相关的全部文档。</p> <p>3) 平台化工具的相关留存数据、分析结果数据。</p> <p>(3) 付款方式</p> <p>付款条件说明：在合同签订生效后，达到付款条件起7日内，支付合同总金额的40.00%，交付验收合格后支付合同剩余总金额60%。</p> <p>(4) 其他要求</p> <p>本项目不组织答疑会和现场考察，投标人可根据实际情况自行开展现场考察，投标人考察现场所发生的一切费用由投标人自行承担。</p> |
|--|--|--|

采购包2：

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

标的名称：网络安全管理运营服务

| 参数性质 | 序号 | 技术要求名称 | 技术参数与性能指标 |
|------|----|--------|--|
| | | | <p>采购包2采购需求</p> <p>1.1采购项目概况</p> <p>省级数字政府已经建立起“政府主导、专业合作、责权清晰、监督有力”的数字政府一体化安全运行保障技术平台（即陕西省数字政府网络安全协调指挥及防控运营平台），监测覆盖部分省级数据中心机房。本项目通过采购安全监测服务，覆盖省级政务云机房和云内安全业务应用，实现全方位的安全风险监测和溯源定位，建立统一的日志审计服务平台，并针对各种需求提供日志服务，配合平台和工具采购网络安全管理运营服务，及时发现、预警和处置问题，在网络安全风险管理层面做到可看、可管、可控。</p> <p>1.2服务内容及服务要求</p> <p>1.2.1服务内容</p> <p>采购包预算金额（万元）：1629.47</p> <p>采购包最高限价（万元）：1629.47</p> <p>供应商报价不允许超过标的金额</p> <p>（招单价的）供应商报价不允许超过标的单价</p> |

| 序 号 | 标的名称 | 数 量 | 标的金额 (万元) | 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 | 网络安全管理 运营服务 | 1 | 1629.47 | 项 | 软件和信 息技术服务业 | 否 | 否 | 否 | 否 |

采购服务内容清单

| 序号 | 服务名称 | 数量 | 单位 | 备注 |
|----|---------------|----|----|------|
| 1 | 安全监测提升服务 | 1 | 项 | 10个月 |
| 2 | 政务云安全监测引擎服务 | 1 | 项 | 10个月 |
| 3 | 公共支撑日志采集服务 | 1 | 项 | 10个月 |
| 4 | 公共支撑日志预处理服务 | 1 | 项 | 10个月 |
| 5 | 公共支撑日志审计服务 | 1 | 项 | 10个月 |
| 6 | 平台设备扩容服务 | 1 | 项 | 10个月 |
| 7 | “三高一弱”重点检查服务 | 1 | 项 | 7个月 |
| 8 | 安全能力评估验证服务 | 1 | 项 | 7个月 |
| 9 | 网络安全风险评估服务 | 1 | 项 | 7个月 |
| 10 | 应急预案服务 | 1 | 项 | 7个月 |
| 11 | 应急演练服务 | 1 | 项 | 7个月 |
| 12 | 安全事件应急响应服务 | 1 | 项 | 7个月 |
| 13 | 安全资产管理服务 | 1 | 项 | 7个月 |
| 14 | 互联网安全资产测绘服务 | 1 | 项 | 7个月 |
| 15 | 安全策略运营服务 | 1 | 项 | 7个月 |
| 16 | 脆弱性采集及闭环管理服务 | 1 | 项 | 7个月 |
| 17 | 基线检查服务 | 1 | 项 | 7个月 |
| 18 | 安全编排与自动化响应服务 | 1 | 项 | 7个月 |
| 19 | 安全事件协助处置服务 | 1 | 项 | 7个月 |
| 20 | 网络安全威胁监测服务 | 1 | 项 | 7个月 |
| 21 | 安全风险资讯预警服务 | 1 | 项 | 7个月 |
| 22 | 本地情报运营服务 | 1 | 项 | 7个月 |
| 23 | 应用上线评估服务 | 1 | 项 | 7个月 |
| 24 | 应用安全监测服务 | 1 | 项 | 7个月 |
| 25 | 重大活动安全保障和值守服务 | 1 | 项 | 7个月 |
| 26 | 安全工单闭环服务 | 1 | 项 | 7个月 |
| 27 | 攻防演练及组织服务 | 1 | 项 | 7个月 |
| 28 | 渗透测试服务 | 1 | 项 | 7个月 |
| 29 | 安全培训服务 | 1 | 项 | 7个月 |
| 30 | 数据风险监测分析服务 | 1 | 项 | 7个月 |
| 31 | 接口安全监测工具服务 | 1 | 项 | 7个月 |

| | | | | |
|----|-----------|---|---|-----|
| 32 | 数据安全管理服务 | 1 | 项 | 7个月 |
| 33 | 供应链安全评估服务 | 1 | 项 | 7个月 |
| 34 | 源代码安全审计服务 | 1 | 项 | 7个月 |

1.2.2服务目标

- 服务项目数：不少于34项；
- 重大活动安全保障服务，年度重保值守不少于7次；
- 渗透测试服务报告交付不少于140份；
- 应用上线评估报告交付不少于15份；
- 现场培训不少于1次；
- 攻防演练组织不少于1次；
- 网络安全服务交付率100%；
- 服务期间平台整体可用性不少于99.9%；
- 服务期间所有租用工具故障率不高于0.1%；
- 工具需求响应交付时间指标不高于1个月；
- 安全监测服务和统一日志服务周期10个月
- 网络安全管理运营服务周期7个月；
- 服务响应时长不高于30分钟；

1.2.3服务要求

- 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
- 标的名称：网络安全管理运营服务

1.2.3.1安全监测提升服务

1.2.3.1.1安全监测设备服务

服务期内提供各类安全监测设备服务，详见以下要求。投标需提供所有安全监测设备工具服务方案、工具部署方案、保障方案。

1）威胁监测系统工具服务

服务期内提供威胁监测系统工具服务，工具可通过镜像流量和采集代理的方式采集未覆盖区域的流量，及时发现网内的安全风险，提升安全盲区的监测预警能力，本次项目提供威胁监测系统工具≥19台（其中10Gbps实网监测性能工具≥11台，20Gbps实网监测性能工具≥6台，40Gbps实网监测性能工具≥2台），所提供的威胁监测系统工具符合需采集区域的网络流量采集性能需求，能够和现网协调指挥平台联动，符合数字政府国产化要求，为国产化硬件工具产品，可存储审计日志天数≥180天，具备≥4个千兆电口、≥6个万兆光口，双冗余电源，10G工具需满足≥128G内存，≥12T存储空间；20G工具需满足≥128G内存，≥16T存储空间；40G工具需满足≥256G内存，≥24T存储空间。

所提供的威胁监测系统工具能力需满足：支持对SQL、XSS攻击等的智能语义分析能力；能够实时发现Web攻击、恶意文件攻击、可疑流量、后门访问、挖矿行为、扫描行为、暴力破解、漏洞攻击、邮件社工类攻击等常

见攻击行为，供攻击者、受害者维度等多维视角聚合分析，自动识别出攻击者的攻击总次数以及攻击行为是否成功；提供威胁情报分析能力，可对分析出的挖矿、隧道通信、远控等攻击进行分类展示，可快速进行问题主机筛选；提供常见协议登录行为审计能力，对可能存在的弱口令、密码明文传输等风险进行告警；提供病毒检测能力和沙箱分析能力，可准确发现未知威胁，并结合云端威胁情报联动确定恶意样本文件中可能存在的安全风险和攻击行为；提供攻击样本的全量分析能力，还原攻击样本的基本信息、进程行为、网络行为、文件行为、注册表行为等攻击行为；提供对网络流量异常的监控能力，可发现网络重传、RESET包异常等异常，可自定义告警判定条件；提供告警抑制能力，可根据现场情况自定义配置抑制周期、抑制阈值、抑制规则；能够基于多种维度进行多维视角聚合分析，识别攻击总次数以及攻击行为是否成功；提供安全场景分析能力，至少包括对勒索病毒、弱口令、挖矿等常见安全场景，可统计展示风险详情、TOP受害者、告警次数等信息；提供智能安全助手，实现告警分析、智能问答等；提供攻击链路可视化能力，可一键溯源查看攻击链条，以图形化形式展示攻击者在网络中的活动路径、攻击过程；提供真实MAC关联能力，可联动获取IP和MAC地址之间的真实关联关系。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

2) 漏洞扫描系统工具服务

服务期内提供漏洞扫描系统工具服务，对各数据中心的云网基础设施设备、云主机、应用、数据库等进行全面扫描与分析，提升安全盲区的漏洞预警能力。本次项目提供部署漏洞扫描工具 ≥ 8 台，均支持不限制地址、域名扫描能力，具备系统、数据库、Web、基线、弱口令等扫描能力，未来可扩展容器安全扫描能力，所提供的漏洞扫描工具符合需部署的数据中心部署需求，能够和现网协调指挥平台联动，符合数字政府国产化要求，为国产化硬件工具产品，可存储审计日志天数 ≥ 180 天，具备 ≥ 4 个千兆电口、 ≥ 2 个万兆光口，双冗余电源， $\geq 32\text{G}$ 内存， $\geq 12\text{T}$ 存储空间。

所提供的漏洞扫描系统工具能力需满足：支持弱口令扫描、系统漏洞扫描、Web漏洞扫描、数据库漏洞扫描和安全基线配置核查等综合漏洞风险扫描功能；兼容CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞知识库；知识库支持自定义编辑，可编辑修改默认的漏洞描述、修复建议、漏洞等级等内容；支持常见Web漏洞类型的扫描，可根据实际需要默认漏洞等级进行自定义修改；支持代理扫描，可通过代理完成云内隔离环境扫描；支持扫描控制功能，在对目标网站扫描时能够设置限制条件或启用智能流控，包括但不限于接收发送速率、并发连接数、最大发送请求数等；支持漏洞反馈，在发现可能的误报后，可直接在扫描结果处进行漏洞的误报反馈。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

3) 全流量采集工具服务

服务期内提供全流量采集工具服务，对网络中重点区域流量数据进行实时捕获和全量存储，实现原始流量数据真实一比一存储回溯分析。本次项目提供全流量采集工具 ≥ 11 台，（其中5Gbps实网性能工具 ≥ 3 台，10Gbps实网性能工具 ≥ 6 台，20Gbps实网性能工具 ≥ 2 台），所提供的全流量工具需符合需采集流量的网络区域网络全流量采集性能需求，能够和现网协调指挥平台联动，符合数字政府国产化要求，为国产化硬件工具产品，可存储会话日志、访问日志等原始流量日志 ≥ 180 天，所有工具均 ≥ 4 个千兆电口、 ≥ 6 个万兆光口， $\geq 128\text{G}$ 内存， $\geq 190\text{T}$ 硬盘，双冗余电源。

所提供的全流量采集系统工具能力需满足：具备物理环境和云环境下的全流量解析和存储回放能力，对加密流量的识别和解密后分析，实现对网络流量的全面捕获和分析；支持对流量中传输的文件进行识别和还原，包括常见的文件格式类型，可辅助样本采集系统进行网络中文件数据的采集；支持对历史数据流量、实时流量的分析，基于指定条件进行图形化呈现，直观展示数据包的构成比例、动态变化趋势，以此来判断掌握网络和业务应用的运行情况，帮助管理人员掌握网络的状态和变化趋势；支持深度分析包括网络协议、网络应用、带宽使用率、流量占比、流速情况、会话情况，能对网络数据包字节分布、传输时延、重传包、同步包数、同步确认包数、重

置包数、广播流量、组播流量等数据指标；支持对不同日期不同时间段网络流量情况对比分析，直观展示分析和网络诊断，覆盖应用层、传输层、网络层、数据链路层等层面常见问题，附带错误描述、问题原因、解决方案等；支持对实时流量、历史流量、历史会话、常见协议访问的回溯和分析，可基于不同时间跨度、时间颗粒度、网络流量、平均包长、IP会话、TCP会话、UDP会话、新建会话等数据类型对网络流量进行回溯和分析；支持对指定时间段内的网络访问情况、会话情况、协议访问日志、应用行为日志、原始访问数据包等进行回溯和分析；支持基于IP、物理地址、网络应用、会话、端口、境外外联访问等多种维度进行全包回溯和分析，包括对网络访问的源地址、目的地址、端口、上下行流量、总流量、上下行数据包数、包长度、三次握手时间、连接失败次数、连接失败率、连接建立时间、响应时延、丢包数、TCP同步包、重复确认包、重置包等参数全方位查看和分析；支持对指定协议、地址、端口、应用、数据包长的数据进行过滤，对不同文件类型的文件开启文件还原，实现文件溯源分析；支持对DNS、HTTP、HTTPS、FTP、Telnet、邮件、数据库、帐号登录行为、SMB、SSH等协议或行为的单独审计记录，关联至原始报文进行回溯分析；系统支持对HTTP访问请求头、请求体、响应头、响应体的全量记录、分析查询和导出；支持对流量数据异常检测和预警，快速发现流量、基线、黑名单、可疑域名访问、可疑邮件标题与内容、可疑特征值流量等异常行为。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

4) 攻击样本采集系统工具服务

服务期内提供攻击样本采集系统工具服务，基于欺骗式防御技术，诱导攻击者深入攻击，隐匿和保护真实的业务系统，实现主动防御。可联动威胁监测系统工具将攻击样本采集系统捕获到的可疑文件进行沙箱深度检测分析。本次项目提供攻击样本采集工具≥8台，所提供的攻击样本采集系统工具需符合需采集的网络区域部署需求，能够和现网协调指挥平台联动，符合数字政府国产化要求，为国产化硬件工具产品，可存储审计日志天数≥180天，具备≥4个千兆电口、≥4个千兆光口，≥2个万兆光口，双冗余电源。

所提供的攻击样本采集系统工具能力需满足：支持对每个采集节点的CPU、内存、存活状态等进行集中监测，以及完成集中停止、重启、重置等操作，提供节点在线远程登录管理能力；能提供丰富的主动防御场景供常见环境快速部署；提供仿真数据构造能力，可构造虚假仿真数据放入采集节点；提供自动学习能力，可学习和伪装真实业务网站页面，诱导攻击；提供攻击行为全面记录，包含攻击者执行的操作命令和日志，在线回放查看攻击的数据包、视频、截图等，便于全方位感知攻击过程，攻击取证，以常见文本格式导出攻击事件和报告，以PCAP格式导出攻击相关流量数据包；提供攻击反制和追踪能力，可识别攻击者的操作系统、终端、网络、手机号码、社交身份信息、邮箱等关键信息，提供反制诱饵文件实现常见系统环境下的反制溯源。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

5) 专业镜像分流工具服务

服务期内提供专业镜像分流工具服务，能够复制接入的网络流量并将其复制传输到不同指定端口，实现镜像流量复用，节约网络镜像资源，本次项目提供≥11台镜像分流工具，镜像分流工具能力要求如下：具备≥48个万兆光口，双冗余电源，符合数字政府国产化要求，为国产化硬件工具产品，提供足够的接口资源和分流性能，支持IPv4/IPv6协议下全量数据包复制转发，且能够满足接口满载接入峰值流量情况下的流量复制转发性能要求；支持接入不限制端口数量的镜像接口，以及不限制端口数量进行流量复制输出，实现任意比例的流量接入、复制输出；支持IPv4/IPv6协议下的五元组包过滤能力；支持剥离特殊数据报文包头，包括但不限于MPLS、GRE、VLAN等，支持报文长度切片和裁剪；支持历史和实时流量统计能力。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

6) 非结构化数据监测工具服务（试点）

服务期内提供非结构化数据监测工具服务（试点），试点梳理和分析流量中传输的非结构化数据，对非结构化数据流转和异常行为进行识别和审计。本次项目提供试点非结构化数据监测工具 ≥ 3 台，所提供的非结构化数据监测工具需符合需采集的网络区域流量性能需求，能够和现网协调指挥平台联动，符合数字政府国产化要求，为国产化硬件工具产品，可存储审计日志天数 ≥ 180 天，具备 ≥ 4 个千兆电口、 ≥ 6 个万兆光口，双冗余电源， $\geq 36T$ 存储空间， $\geq 128G$ 内存， $\geq 10G$ 检测能力。

所提供的非结构化数据监测工具能力需满足：支持指定网络流量和请求方法的审计和过滤；可识别常见Office、WPS类办公文件、图片、压缩文件、网页文件、文本文件、图纸、代码等常见非结构化数据类型，支持红头文件、印章识别；支持对常见身份证、银行卡号、手机号、邮箱等敏感内容识别；支持异常高频访问、非工作时间操作等敏感行为识别，可自定义异常行为判定条件配置；支持基于预设条件对敏感数据行为提供告警、审计，支持敏感数据跨域、跨境流转分析；支持对上传的指定文件生成文件指纹，实现指定文档识别；支持数据泄露分析，可基于对告警、风险文件、IP地址、邮箱等多种维度进行分析；支持记录告警和审计日志，可基于特定条件进行筛选查看和导出。投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

1.2.3.1.2安全监测设备工具保障要求

为本项目所提供的124台安全监测设备工具、原有平台相关前置系统162台，共计约286台服务工具，在服务期内提供基础保障，包括但不限于定期巡检、按需升级、故障处理、告警处理、日常运维操作、日常管理等保障，保障相关工具能够正常稳定运行。

定期巡检：每周对安全工具设备进行一次远程巡检，需要登录对设备检查，填写检查记录表，在巡检完毕后，填写《巡检表格》，每月对位于省级各数据中心的相关安全工具设备、每年对位于各地市的省级配发安全工具设备进行一次现场巡检，检查工具物理状态和运行状态，在巡检完毕后，填写《巡检报告》。同时，对巡检过程中发现的重大问题，及时上报采购人相关管理人员，并进行问题处理。运行状态检查内容包括但不限于：CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况、电源状态、物理运行状态等运行状态相关的基本参数。

定期升级：对相应设备进行版本或特征库升级，保证系统处于最新状态，同类设备的系统版本和特征库版本保持一致。

故障处理：进行日常5×8小时的驻场值守保障，以及7×24小时的工具故障响应，当工具出现故障时，协助厂商进行故障处理操作，并视情况协调相应的厂商工程师到现场进行进一步故障处理和修复，当安全设备出现硬件故障时，联系厂商完成备品备件更换，备品上架、故障设备返厂等工作。

告警处理：进行日常5×8小时的驻场值守保障，当发现工具设备系统告警事件时，立即对告警事件进行确定、排查、分析和处理，必要时可联系厂商进行现场处置，确保设备的运行稳定。

日常运维操作：进行日常5×8小时的驻场日常运维操作，对设备进行各类日常操作、后台维护、日常维护等运维工作，确保设备能够完整的达成预定的数据采集目标、完成日常数据采集任务，能够正常的为现网平台提供数据支撑。

日常管理：驻场人员在采购人指定的场地进行办公，日常进行设备的相关管理操作，包括但不限于设备管理、运维管理、工具技术支撑、技术答疑等。

1.2.3.2政务云安全监测引擎服务

服务期内提供政务云安全监测引擎服务，提供服务工具构建当前数据中心的云安全监测资源池和监测服务目录，提供重点业务系统云内安全监测服务和云内安全工具应急响应能力，并可按需扩展服务能力。本次项目所提供的云内安全监测工具服务资源池应能覆盖省信息化中心机房、西咸信创云数据中心、西咸联通主数据中心的政务外网、政务互联网，服务工具需分布式部署在各数据中心的云平台区域，并通过主节点实现各数据中心子节点

统一管理，能够和现网协调指挥平台联动实现云内安全监测数据采集、汇集，工具需符合国产化要求，兼容政务云VPC隔离环境，非开源工具，满足国产芯片+国产操作系统要求。

为本项目所提供的日志服务工具在服务期内提供基础保障，包括但不限于定期巡检、按需升级、故障处理、告警处理、日常运维操作、日常管理等保障，保障相关工具能够正常稳定运行。具体要求参考安全监测设备工具保障要求。**提供政务云安全监测引擎服务方案、工具部署方案、保障方案。**

服务工具应符合数字政府国产化要求，具备良好的网络扩展性，单台工具提供≥4个万兆光口，≥8个千兆电口，≥48核心，≥384G内存，≥48T硬盘空间。总计提供物理核≥720核心，内存≥5760GB，硬盘空间≥720TB，提供≥150个云内安全监测组件的接入能力，可提供≥100Mbps、≥500Mbps、≥1Gbps规格的云内安全监测引擎，后期可持续平滑扩展资源池规模，不影响集群正常运行。

▲工具支持能力如下：**1.统一管理：**服务工具提供云内安全监测组件统一安全管理能力，可以对所提供的所有云内安全监测组件进行统一管理和分析，提供统一配置、故障告警、性能、安全、报表等安全管理能力，可联动现网协调指挥平台对云内采集的各类安全事件进行集中采集和智能分析，实现对云内安全风险的统一监控分析和预警处理。**2.统一用户：**支持面向用云业务单位、省数政局、省数政中心开通用户，用户体系同步自现网统一认证平台，可实现一个用户对分布在不同数据中心的业务安全统一管理。**3.业务单位管理：**支持对不同单位按需分配不同规格的云内安全监测组件，用云业务单位可通过自助工单形式申请云内安全监测服务，经过管理员审批即可使用。支持临时应急成员，可在应急时设置临时账号和应急有效期，在有效期内使用相关安全组件完成应急。**4.数据隔离：**各单位用户只能看到本部门（单位）的安全监测情况，实现安全数据的隔离。**5.组件自动部署：**实现云内安全监测组件的一键开通并自动化部署，支持按需申请-审批方式合理分配安全资源。在开通安全监测组件时，可自助选择开通的性能规格、有效周期等信息，提交完成审批后可实现云内安全监测服务的自动激活，无需人工干预。**6.组件管理：**支持云内安全监测组件管理能力，可在线管理已开通的云内安全监测组件，并实现组件单点登录、状态自动巡检。**7.应急支撑：**支持应急开通防火墙、漏洞扫描、WAF、网页防篡改、堡垒机、日志审计、主机安全、数据脱敏、数据库防火墙等应急支撑能力，可在线管理应急支撑组件，并支持单点登录相应组件。**8.协调指挥平台对接单点登录：**与现网协调指挥平台定制对接，协调指挥平台用户可一键单点登录到云内安全监测服务工具，并通过工具统一管理权限范围内的云内安全监测组件。**9.可视化：**支持可视化展示，支持基于云内安全监测采集的数据综合呈现云内整体安全态势情况，并呈现单用户视角云内安全态势。投标需提交工具除对接开发要求外的所有能力证明材料，不限产品截图、官网说明、第三方证明材料等。

▲云内安全监测组件能力要求如下：支持对SQL、XSS攻击等的智能语义分析能力；能够实时发现Web攻击、恶意文件攻击、可疑流量、后门访问、挖矿行为、扫描行为、暴力破解、漏洞攻击、邮件社工类攻击等常见攻击行为，供攻击者、受害者维度等多维视角聚合分析，自动识别出攻击者的攻击总次数以及攻击行为是否成功；提供威胁情报分析能力，可对分析出的挖矿、隧道通信、远控等攻击进行分类展示，可快速进行问题主机筛选；提供常见协议登录行为审计能力，对可能存在的弱口令、密码明文传输等风险进行告警；提供病毒检测能力和沙箱分析能力，可准确发现未知威胁，并结合云端威胁情报联动确定恶意样本文件中可能存在的安全风险和攻击行为；提供攻击样本的全量分析能力，还原攻击样本的基本信息、进程行为、网络行为、文件行为、注册表行为等攻击行为；提供对网络流量异常的监控能力，可发现网络重传、RESET包异常等异常，可自定义告警判定条件；提供告警抑制能力，可根据现场情况自定义配置抑制周期、抑制阈值、抑制规则；能够基于多种维度进行多维视角聚合分析，识别攻击总次数以及攻击行为是否成功；提供安全场景分析能力，至少包括对勒索病毒、弱口令、挖矿等常见安全场景，可统计展示风险详情、TOP受害者、告警次数等信息；提供智能安全助手，实现告警分析、智能问答等；提供攻击链路可视化能力，可一键溯源查看攻击链条，以图形化形式展示攻击者在网络中的活动路径、攻击过程；提供真实MAC关联能力，可联动获取IP和MAC地址之间的真实关联关系。投标需提交工具除对接开发要求外的所有能力证明材料，不限产品截图、官网说明、第三方证明材料等。

1.2.3.3公共支撑日志采集服务

服务期内提供公共支撑日志采集服务，通过日志服务平台工具覆盖各省级数据中心和云网基础设施，为云网基础设施和各用云业务单位提供高性能日志采集服务，中标服务方需配合测评公司完成服务工具平台的网络安全等级保护第三级测评、商用密码应用安全性评估第三级测评。

所提供的日志服务平台工具集群部署于省级数据中心的政务外网和政务互联网区域，其中政务外网集群节点≥10个，互联网集群节点≥8个，并能通过网闸完成受控数据交互。所提供的日志服务集群工具符合日志采集的高性能、高可用、高并发需求，符合数字政府国产化要求，兼容政务云VPC隔离环境，可存储审计日志时长满足采购人需求。政务外网集群不限制日志源接入授权数量，具备良好的网络扩展能力，单台工具节点提供≥4个千兆电口，≥4个万兆光口，总计提供≥320物理核、≥1280GB内存，≥900TB存储空间，≥30wEPS日志采集接入能力，后期可持续平滑扩展集群规模，不影响集群正常运行；政务互联网集群不限制日志源接入授权数量，具备良好的网络扩展能力，单台工具提供≥4个千兆电口，≥4个万兆光口，总计提供≥256物理核、≥1024GB内存，≥700TB存储空间，≥24wEPS日志采集接入能力，后期可持续平滑扩展集群规模，不影响集群正常运行。投标人需配合提供日志服务平台组网所需交换机，≥2台，单台交换机≥24万兆光口，性能满足使用需求。

本次项目除日志平台集群外，还需提供≥6台日志分布式采集工具，对不同区域的日志数据进行本地集中采集和转发，采集器需支持集中管理和策略下发，为硬件独立产品，国产化芯片+操作系统，支持云内日志采集代理能力，单台采集器工具的采集和转发速率≥50000EPS，不限制接入日志资产数，接口≥2个万兆光口，≥4个千兆电口，硬盘空间≥20T，内存≥64G。

▲日志服务工具需满足：**1.节点高可用**：提供多节点部署和高可用能力，当某一日志节点宕机后可自动负载至其它节点，不影响日志服务正常运行，确保日志服务的连续性。支持自动恢复机制，故障节点如果因为软件问题宕机，有自检机制能够记录当时的异常情况并自动恢复服务，在服务恢复后，可自动重新加入集群并恢复服务。**2.数据高可用**：提供日志数据高可用能力，在存储节点宕机后，数据不会丢失，确保日志服务的连续性和稳定性；支持平台备份外发日志至延安灾备中心，当需要查询历史数据时，可恢复指定日期数据进行查询。**3.节点动态扩容**：提供动态扩展能力，可在不停机情况下增加日志服务节点，对CPU、内存、存储空间等资源进行动态扩展。**4.政务云VPC内部日志采集**：提供各数据中心政务云内部多VPC环境日志采集能力，对各用云业务单位的VPC内部日志数据进行汇聚，集中转发至日志平台进行处理，并可区分识别各VPC内部重复的IP资产日志。**5.第三方日志接入对接**：服务期内免费提供与第三方平台、系统的日志接入对接服务，实现第三方平台、系统灵活接入。**6.灵活的日志采集接收能力**：提供灵活的日志采集能力，实现对各类操作系统、云平台、云主机、数据库、中间件、应用系统等日志采集，提供多种常见协议方式进行日志数据采集，包括但不限于API、SYSLOG、SNMP、FTP、WMI、ODBC等常见方式，提供日志采集代理、Agent客户端采集等方式。Agent兼容信创环境，可直接安装并运行在云主机等审计对象上，实现对审计对象的日志数据采集和转发，Agent采集的日志可转发给日志采集代理。投标需提交工具除对接开发要求外的所有能力证明材料，不限产品截图、官网说明、第三方证明材料等，并说明投标工具的节点高可用、数据高可用、动态扩容能力实现原理和机制。

服务期内为所提供的日志服务工具提供基础保障，包括但不限于定期巡检、按需升级、故障处理、告警处理、日常运维操作、日常管理等保障，保障相关工具能够正常稳定运行。具体要求参考安全监测设备工具保障要求。

提供公共支撑日志采集服务方案，内容需覆盖工具技术架构介绍、功能介绍、工具部署方案、保障方案。

1.2.3.4公共支撑日志预处理服务

服务期内提供不限次公共支撑日志预处理服务，按需提供数据预处理支撑工作，支撑其它数据需求平台、系统、单位等获取高质量的标准日志数据。提交日志格式标准、预处理报告、数据处理报告。

服务期内需协助采购人制定统一日志数据格式标准，作为统一日志存储和共享利用标准，日志服务工具的采

集、存储、处理的日志格式均遵循此标准开展。

服务期内需安排专人驻场对已采集的日志原始数据进行分析，遵循统一日志数据格式标准，制定日志预处理规则，结合日志工具完成各类采集日志的数据清洗、聚合、拆分、过滤、补全、标准化转换等数据预处理工作，完成日志的预处理工作，完成预处理后的日志方可入库存储和供日志查询共享使用，提供标准数据支撑。还需基于日志的查询、处理、分析等场景进行常态化观察和分析，基于分析结果，完成日志预处理规则的优化和后台日志索引优化，提升日志处理效率。

服务期内需提供专人驻场提供数据预处理支撑，按数据需求方提出的日志需求进行日志数据的预处理，按需开展数据预处理工作，包括但不限于数据清洗、富化、打标、映射、提取、查询统计、函数计算等，并以不同方式方法（包括但不限于API、SYSLOG、FTP等）提供治理后的日志数据供外部调用、查询、利用，处理后的数据满足数据需求方对日志数据的利用需求和质量要求，满足日志接口查询调用需求。

需按要求提供服务方案。

1.2.3.5公共支撑日志审计服务

服务期内基于日志服务工具为各方提供日志审计服务，面向各单位提供SaaS化日志服务，至少满足≥100个日志单位用户使用需求，需面向不同单位用户，设计不同的日志数据、菜单和角色权限，可支持的总日志源规格授权不限，面向各日志需求单位提供不少于6种日志服务规格。

▲面向各业务单位所提供的日志审计服务需满足：**1.独立管理能力**：为各单位提供独立的日志服务登录管理入口，可登录管理日志工具，并进行相关操作，权限限定为各业务单位自身数据权限。**2.协调指挥平台对接单点登录**：与现有协调指挥平台定制对接，协调指挥平台用户可一键单点登录到日志服务工具自身权限对应的日志工具用户，完成管理操作、查询等。**3.关联分析能力**：提供关联分析能力，可基于行为模型进行场景化分析，各方可基于自身需求进行自定义分析，包括但不限于失陷主机、异常登录、非法访问、设备异常等分析。**4.数据可视化能力**：提供日志数据可视化分析能力，可面向各单位提供可视化能力，采用仪表盘、柱形图、折线图、明细表、地图等方式对日志数据信息进行排布和可视化呈现。**5.查询分析能力**：提供历史日志数据查询分析能力，可基于多维查询条件组合查询，并实现日志结果数据分析和导出。投标需提交工具除对接开发要求外的所有能力证明材料，不限产品截图、官网说明、第三方证明材料等。

面向采购人所提供的日志服务能力需额外满足：**1.统一用户**：支持面向采购人、各业务单位开通用户，用户体系同步自现网统一认证平台，可实现单用户对分布在不同数据中心的日志数据实现统一管理。**2.灵活权限管理**：提供灵活权限管理能力，将菜单权限绑定角色，数据权限绑定用户，只允许用户访问允许访问的菜单和自身权限数据，防止越权访问。面向采购人的高权限管理账户可看到和管理所有用户日志数据。**3.日志场景分析服务**：服务期内提供日志场景化分析服务，提供≥5个场景分析，建立场景分析模型，覆盖常见业务场景分析，实现异常预警、日志综合分析利用。

服务期内为所提供的SAAS日志审计服务能力提供技术保障，保障相关单位能够正常使用日志服务能力，对提供的日志审计能力提供技术支撑、技术答疑。

提供公共支撑日志审计服务方案，内容需覆盖日志功能介绍、日志场景分析模型方案、保障方案。

1.2.3.6平台设备扩容服务

服务期内面向现网数字政府网络安全协调指挥平台和防控运营平台提供平台设备扩容服务，协调指挥平台扩容≥12台服务器，防控运营平台扩容≥2台服务器，服务期内需确保扩容后平台性能满足采购人日常使用需求，若不足，则需要根据实际情况扩容至满足需求，提供相关承诺函。

新扩容服务器工具兼容现网服务器集群，单台服务器需满足标准2U机架式设备，双电源，提供国产化CPU及操作系统，提供CPU核数≥64核，≥256GB内存，≥48T硬盘存储空间，支持RAID0/1/5/6，提供千兆电口≥4个，万兆光口≥4个，能够满足两大平台的部署和运行所需，每台服务器MTBF(平均无故障工作时间)≥60000小时，



1

采购内容及要求

硬件服务器年度稳定运行率 $\geq 99.9\%$ ，系统故障平均间隔时间： ≥ 180 天，系统单次故障恢复时间 ≤ 1 小时。

对原有服务器集群，每台服务器扩展 ≥ 4 万兆光口接口，完成新扩容服务器工具与原有服务器集群的集群扩容升级工作。

面向现网数字政府网络安全协调指挥平台和防控运营平台提供合规保障服务，包括但不限于数据库合规改造、国密改造适配、维保续期、定期巡检、组件升级、故障处理、告警处理、日常运维操作、日常保障等，保障平台正常稳定运行。具体如下：

数据库合规改造：需对两大平台的集中式数据库使用情况、数据情况等进行充分调研和技术论证，采用目前较为成熟稳定的集中式数据库软件，对平台进行集中式数据库的替代，替代原有非国产集中式数据库，完成两大平台集中式数据库的国产化适配、迁移、上线，并做好原有数据迁移计划、迁移方案。

国密改造适配：按要求提供服务期内有效的平台国密SSL证书，并配合完成两大平台国密SSL证书的适配、兼容和上线使用，实现国密+国际双证书，实现平台的高强度SSL加密连接及身份认证。

维保续期：服务期内对平台的软件维保进行续期，保障平台的稳定运行，且组件处于最新状态，不存在严重安全风险隐患和漏洞。

定期巡检：每天对平台运行状态、使用状态、服务状态等进行远程检查，确保平台正常稳定运行，输出平台状态巡检表，对巡检过程中发现的重大问题，及时上报采购人相关管理人员，并进行问题处理。每月进行现场巡检工作，检查内容主要包括：CPU使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等运行状态相关的基本参数。

升级：定期对平台进行组件和版本升级，确保平台的各组件版本以及平台自身不出现由于自身脆弱性导致的安全风险，联系平台开发厂商对平台的功能版本进行维护，对升级过程和结果进行记录。

故障处理：提供日常5×8小时的驻场值守保障，7×24小时的平台故障响应，确保能够及时响应和快速解决平台的各类故障，并确保平台的运行支撑环境稳定。

告警处理：进行日常5×8小时的驻场值守保障，及时对平台自身产生的系统告警、服务告警等情况进行处理，必要时联系平台厂商进行协同处置，确保平台的正常运行不受告警影响。

日常运维操作：进行日常5×8小时的日常运维操作，对平台进行后台管理、数据维护、维护操作等运维工作，确保平台能够完整的达成预定的使用目标、功能和流程能够正常、完整的运行和流转。

日常保障：平台保障人员在采购人指定的场地进行办公，每周工作日5×8小时不间断的进行保障服务，为平台用户提供服务请求响应、技术咨询支持服务。

提供扩容承诺函和平台设备扩容服务方案，内容需覆盖平台扩容设计方案、实施方案、保障方案。

1.2.3.7“三高一弱”重点检查服务

完成采购人管理的西咸联通主数据中心、西咸广电备数据中心、西咸信创云数据中心、省信息化中心机房、新建高性能政务云、延安灾备中心等基础设施资产、自有业务系统、省级部门的上云业务系统、省级政务外网、省级政务互联网、各地市接入省政务外网广域网边界、省级各部门接入城域网边界24000余个资产的“三高一弱”（高危端口风险、高危行为风险、高危漏洞风险、弱口令风险）重点威胁专项检查，服务期内检查次数 ≥ 2 次；对发现的高危风险通过协调指挥与防控运营平台发布安全通报、整改通知、完成整改修复后的二次验证，形成闭环管理；交付实时的提醒单、风险汇总表；提交实施方案、专项报告、总结报告。基于检查积累的经验和成果，对现网协调指挥平台的漏洞管理功能进行调优，调优实现漏洞批量管理、一键复测。

1.2.3.8安全能力评估验证服务

完成采购人管理的西咸信创云数据中心、西咸联通主数据中心政务互联网和政务外网边界的安全能力评估验证。以人工服务加专业技术工具的方式，结合安全风险场景威胁建模、自动化评估脚本、仿真评估环境等多种方

式方法，完成数字政府当前边界、横向的安全防御、监测、响应能力的有效性验证。

评估内容至少覆盖暴力破解、病毒防护、web shell上传、横向攻击、远控木马、黑客后门代理（持久化）、注入攻击、命令执行、绕过攻击、常见漏洞攻击行为、访问恶意URL、下载恶意样本等场景；

▲投标人自备专业评估工具，提供工具必须具备国产化等通用环境部署能力，检测结果指标化；具备自动化模拟攻击检测能力，实现基于路径（渗透攻击、漏洞攻击、横向移动、边界突破等）、命令执行、攻击等级、攻防战术技术、攻击阶段、关联方法等能力。可查看等级分布、防御成功率及分布、攻击用例数、已检未检统计、攻防战术技术统计及矩阵等内容和报告；通过监测代理组件采集信息，并可上传相关监测设备结果综合分析；对发现的问题需完成复测的闭环管理。

需提交以上功能证明材料，不限产品截图、官网说明、第三方证明材料等。服务期内≥1次服务，提交实施方案、详细评估报告。

1.2.3.9网络安全风险评估服务

完成采购人管理的核心系统及上云重要应用系统从资产威胁、弱点、影响、衍生风险多个维度评估，从安全技术和管理方面，按照国标完成风险评估，输出评估报告（含方案、报告、过程资料），并在协调指挥与防控运营平台在线流转，对风险修复结果进行二次验证。服务期内评估系统≥15个，服务期内每系统评估不少于1次。基于风险评估经验和过程，对现网防控运营平台功能进行调优对风险评估服务开展情况、进度、成果展示能清晰展示，实现服务进度、过程、结果的管理和呈现。

1.2.3.10应急预案服务

完成采购人管理的核心业务应用系统的应急预案，应急场景至少包括黑客攻击成功应急、失陷主机应急、数据泄露事件应急、数据篡改事件应急、业务被攻击中断应急等不同场景，提供不同应急预案；预案不限于事件级别定义、应急组织架构、责任分工、应急流程和办法、预案的执行和实施等内容，明确重大安全事件发生后如何进行快速响应；在协调指挥平台的在线知识库进行预案在线维护管理，按照采购人确认后的流程同步在平台建立应急处置业务流程，流程需在线流转。应急场景化预案不少于5个。基于应急管理需求，对现网协调指挥平台进行调优，实现在线应急场景化管理，可基于平台管理安全应急预案、流程和联系人，衔接应急流程各个角色。

1.2.3.11应急演练服务

完成采购人管理的核心业务应用系统制定的应急预案的演练，通过演练明确各处室责任，检验准备措施、配合机制、各环节配合程度，设立应急演练工作小组，并设置不同角色负责不同职责；模拟各种突发事件场景，搭建模拟仿真业务环境，模拟爆发上述场景事件，以演练提高防范意识和处理能力；交付不限于场景实施方案、总结报告、演练脚本等；每场景演练不少于1次。

1.2.3.12安全事件应急响应服务

协助采购人完成自有62个直管业务系统的安全事件应急响应服务，成立专项应急响应小组提供现场应急响应服务，在网络/数据安全事件触发后，按照应急预案基于事件严重程度，采取不同等级响应处置，溯源、恢复等有效措施；通过应急上报及联络机制，及时得到上级主管部门指导、联系本组织相关人员、响应人员；接到应急需求后，基于事件级别提供应急启动、抑制、根除、恢复、跟进等有效措施；在协调指挥与防控运营平台上完成全流程的流转和记录；应急时间小于采购人要求时限；服务期限内应急总结报告不少于7份，每份报告提交时间小于2天。基于应急响应需求，对现网协调指挥平台进行调优，实现在线应急值班管理、应急联络及调度机制，在线实现应急联络、调度、快处和协同，完成和运维中枢平台对接。

1.2.3.13安全资产管理服务

在采购人建设的协调指挥与防控运营平台完成符合管理要求的资产动态台账，含西咸联通主数据中心、西咸

广电备数据中心、西咸信创云数据中心、省信息化中心机房、新建高性能政务云、延安灾备中心基础设施资产、采购人自有业务系统、省级部门的上云业务系统、省级政务外网、省级政务互联网、各地市接入省政务外网广域网边界、省级各部门接入城域网边界24000余个网络资产的资产管理，利用工具、前置系统、其它资产数据来源等形成资产全生命周期管理，交付不限于实时统计清单、季度及年度清单等，实时更新、汇总归档。服务期内完成与运维管理中枢平台、一体化资源监测和调度管理平台对接，具备IP、系统、单位的对照关系；基于服务过程中的资产管理需求，对现网协调指挥平台的资产管理功能进行调优，增加资产入库认领、确认、变更、退库的全生命周期管理能力，可对新资产进行入库认领、补充信息，二次审批后正式入库，对变更资产二次审批，对退库资产需审批退库，实现资产统一查询，实现弹性公网IP、NAT地址等复杂地址资产与常规IP资产、系统资产的关联。

1.2.3.14互联网安全资产测绘服务

▲完成采购人管理的西咸联通主数据中心、省信息化中心机房的互联网资产测绘，评估其安全风险，基于结果处置影子资产、无主资产、高危风险资产；投标人需自备专用工具，审批后使用；完成资产测绘工作支撑，在协调指挥平台完成信息录入、风险提示、处置反馈和闭环管理等业务；测绘数据含如IPv4/IPv6地址、域名及DNS解析关联、端口服务、指定高危漏洞的分布区域、影响趋势、影响区域及端口排名、域名资产的域名备案及子域名、归属单位、运营商、IP及归属、端口、地理位置、返回标题、历史解析记录等信息、Web框架及开发语言等信息；投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等；服务期内资产测绘数量不少于1500条；交付不限于实施方案、资产汇总清单、季度、年度测绘报告等，需实时更新、汇总归档。

1.2.3.15安全策略运营服务

完成采购人管理的协调指挥与防控运营平台、平台相关前置系统的策略运营，含不同时期（日常、重保等）安全管理、数据汇总分析、用户需求等的策略确认、调整优化，对安全采集工具策略检查、调优，视情况调整监测细粒度、强度等策略；对平台视情况调整分析强度、颗粒度、预警等级、覆盖对象等，提供策略运营报告。

1.2.3.16脆弱性采集及闭环管理服务

完成采购人管理的西咸联通主数据中心、省信息化中心机房、西咸信创云数据中心等省级政务云部署的9000余个云主机资产的按需和专项分析服务，服务含驻场按需服务输出报告、协助指导处置，定期专项监测、扫描、分析、验证、预警、复测等，协助指导处置；对高危脆弱性风险通过人工分析、人工验证、漏洞POC测试等验证后通过协调指挥与防控运营平台下发；交付不限于脆弱性记录表单、相关漏洞报告总结、汇总报告等；实时更新、提醒、汇总归档。

1.2.3.17基线检查服务

完成采购人管理的自有应用系统、上云各业务单位9000余个云主机的按需检查，对申请资产进行抽查，服务期内检查≥400资产；检查内容和标准符合工信部、等级保护等合规要求，含操作系统、数据库、中间件检查等，并将检查结果录入协调指挥平台和协调指挥与防控运营平台，通过平台完成整改通知下发、整改后二次验证；提供检查方案，并按系统或部门交付检查报告、汇总报告。

1.2.3.18安全编排与自动化响应服务

完成采购人管理的各数据中心网络基础设施资产的安全编排与自动化响应服务；对采集的安全数据及常见风险场景归类分析、动态调整、完成分析模型；通过图形化界面拖拽编辑自定义剧本，包括标准动作、设备动作、决策、人工任务、并行节点和等待节点等，配置具体采集节点、审核节点、确认节点等，并指定各节点的归属人、参与人角色、参与人等；通过协调指挥与防控运营平台完成流程建设、实现自动化响应服务；交付不少于5个场景分析设计和不少于5个脚本配置或优化，完成报告输出。

1.2.3.19安全事件协助处置服务

完成各部门上云业务系统5×8小时驻场实时协助处置服务，不限系统数量，提供入侵溯源、处置指导、加固技术指导、建议等，服务期内不限次数；交付成果含协助处置报告、协助处置汇总表等；报告提交时间不超过1周，表单实时更新、汇总归档。

1.2.3.20网络安全威胁监测服务

完成采购人管理的西咸联通主数据中心、西咸广电备数据中心、西咸信创云数据中心、省信息化中心机房、新建高性能政务云、延安灾备中心等基础设施资产、自有业务系统、省级部门的上云业务系统、省级政务外网、省级政务互联网、各地市接入省政务外网广域网边界、省级各部门接入城域网边界24000余个资产的7×24小时网络安全威胁监测服务，服务期限内不少于4人的5*8小时驻场值守监测、其它时间远程监测。监测的风险事件经关联分析、人工验证后，通过协调指挥及防控运营平台发布预警提醒、风险处置、处置反馈、风险处置验证等；因客观原因无法在限定时间内完成处置的，提供风险建议控制措施，并记录归档加强后期监控。交付不限于监测汇总表、重大风险报告、风险提醒单、半月汇总报告、年度汇总报告等；完成实时更新、提醒、汇总归档。服务期内，基于服务过程及经验积累，对现网协调指挥平台的协调指挥模块中的通报、预警、通知功能进行调优，完成包括但不限于界面优化、新增功能如超时延期、撤回等。

1.2.3.21安全风险资讯预警服务

完成采购人管理的各数据中心重要基础设施资产、自有业务系统等相关风险资讯预警；搜集匹配国内外网络安全最新政策、动向、热点资讯、风险漏洞等，每周汇总、整理，输出资讯，基于平台完成风险资讯录入和在线推送。交付不限于资讯周报、年度汇总报告，服务期内周报交付≥30份。服务期内基于服务的开展和问题情况，对现网协调指挥平台的预警、通知功能完成调优，包括但不限于调整功能细节、展示界面、数据呈现方式等。

1.2.3.22本地情报运营服务

完成采购人管理的省数字政府云网基础设施资产、自有业务系统等相关的本地情报运营服务；对日常监测发现的重大风险、攻击源等通过协调指挥与防控运营平台完成上报录入、复核、确认等，完成情报IP、标签、详情，基于平台完成情报的匹配应用、关联联系人/单位预警通告，实现情报利用和共享。交付不限于情报汇总表、汇总报告；提供实时的更新、预警、汇总归档。

1.2.3.23应用上线评估服务

完成采购人及各用云业务单位新上线应用系统的上线安全评估服务，审核业务方提交的自查安全资料，含等级保护测评相关资料、密码应用测评相关资料、渗透测试、漏洞扫描、源代码审计、基线等，使用相关技术手段、工具等完成业务安全架构、安全合规性、脆弱性等评估，提供整体实施方案、对应评估报告；在协调指挥与防控运营平台上完成评估报告上传、风险通知下发、风险处置流转、处置二次验证等流程，确保系统高危隐患、风险可控；服务次数不少于15次，上线评估报告不少于15份。

1.2.3.24应用安全监测服务

▲完成采购人管理的各数据中心、茶张路机房的主要互联网230余个站点的安全监测服务，含站点挂马监测、暗链监测、篡改监测、可用性监测、漏洞监测、敏感内容监测等；提供篡改、暗链、坏页、黑页、挂马等高危事件、取证截图上传及查看；提供分布式节点可用性监测，实现多运营商、多区域、多链路、多点监测的多线路的域名解析、网站访问、IPv4/IPv6可用性访问监测；提供常见Web漏洞、OWASP TOP10漏洞监测，实现高危漏洞、取证截图、漏洞POC验证等上传及查看；提供敏感字、身份信息敏感内容监测；监测结果通过协调指挥与防控运营平台完成闭环管理和结果展示；提供服务期内7×24小时安全风险监测，高危风险验证时间小于8小时；预、告警信息通过秦政通、短信、邮件等多种方式发布；投标人需提交安全监测能力证明材料，不限截图、官网说明、第三方证明材料等；交付不限于每系统月度监测报告、风险问题提醒单、问题汇总表。

服务期内需能根据日常应用安全监测服务的开展情况和使用问题情况，对协调指挥平台的协调指挥模块中的通报、预警、通知模块功能进行调优，包括但不限于调整功能细节、展示界面、数据呈现方式等。

1.2.3.25重大活动安全保障和值守服务

完成采购人管理的各数据中心云网基础设施的重大活动期间（如两会、春节、国庆、护网等）、特殊时期（视采购人安全情况而定）网络安全保障工作，满足重要时期数字政府网络安全保障要求，保障数字政府网络和业务系统正常运行；提供活动前风险自查工作，跟进风险问题处置的二次验证；重保期间通过协调指挥及防控运营平台的重保模块协调相关单位完成重保实时监测。活动期间7×24小时值守对中高风险问题实时监测、预警、处置、复测完成闭环管理，对安全协助需求实时响应，对高危事件即时响应；服务期内重保天数不少于80天；每次重保活动前提交保障方案，活动开始前一周提交；活动完成后提交总结报告，整理报告时间不长于活动结束后一周。

1.2.3.26安全工单闭环服务

按照采购人和省级各部门需求、梳理、设计、优化安全流程模板，提供新流程不少于7个，服务期内更新优化不少于14个流程等，在协调指挥与防控运营平台实现流程在线运行、流转，对安全流程模板持续修订、优化，提供流程设计资料。服务期内提供5×8小时驻场工单服务、7×24小时响应工单闭环服务，通过协调指挥与防控运营平台完成流程工单下发/转派、审核、催办、归档、闭环、管理、资料整理等；采用人工电话、短信、秦政通、平台消息等提醒方式推进工单流转和处置闭环管理。交付不限于月度、年度工单归档汇总报告、流程设计资料等。服务期内基于工单闭环服务需求和遇到的问题，对防控运营平台进行调优，完成工单办理、展示等优化，包括但不限于导出、在线打印、超时延期、撤回、知会等。

1.2.3.27攻防演练及组织服务

完成省政务云部署业务系统、各地市核心业务系统为范围的网络安全攻防演练活动，服务期内开展不少于1次，规模参考同行业活动；提供演练前期筹备含活动策划、印刷设计、环境搭建、现场演练支撑、裁判服务、摄影服务、总结服务等；承担不限于活动相关设备租赁、场地搭建、演练场地租赁、参会人员活动期间食宿、邀请专家、活动奖金、活动纪录片、等费用；提供活动现场和攻击队员的监测、溯源及分析服务，保证攻击过程合法合规，提供活动现场人员的生活保障。组织不少于15支攻击队，每队不少于3名攻击队员；活动裁判不少于3人、现场支撑人员不少于10人；演练开始时间及周期根据采购人需求确定。

▲采购人提供攻防演练平台，平台提供本地或云端部署，配置相关审计及行为监测措施保证攻击行为可记录和追溯；不限于攻防演练管理、实时攻防展示、攻击方仅有成果提交权限（含IP授权申请、成果上传、成绩管理、总结等）、防守方仅有成果提交权限（含攻击IP合法性查询、系统资产管理、成果上传、成绩管理、总结等）、裁判方拥有有限权限（含裁判审核、攻击行为审计、攻防双方成果查看和评分、攻防双方总结查看、攻防双方成绩排名、攻击行为审计结果查看等）；管理方拥有后台管理权限（含总览大屏、攻防双方相关成果大屏，攻防活动相关审计及结果分析等）；投标人需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

攻防演练总结报告中风险通过协调指挥与防控运营平台针对性下发相关单位、提供协助处置、处置结果二次验证等；交付成果不限于演练方案、演练问题通知单、总结报告、攻防归档资料等；投标人需提供全过程文档样例。

1.2.3.28渗透测试服务

完成采购人管理的自有系统、各上云业务单位系统不少于140次系统的人工渗透测试（每系统做一次记数量一次），深度测试、评估、分析业务安全隐患和漏洞可利用程度，输出测试报告并给出处置建议；报告通过协调指挥与防控运营平台在线管理和流转下发，提供风险处置的二次验证；对暂时无法处置风险需给出风险控制建议

和指导，并加强后期监控；测试范围不限于业务相关的移动APP、Web站点、小程序、CS客户端等，测试类型不限于信息收集类、配置管理类、认证类、会话类、授权类、数据验证类、系统应用漏洞等；服务期内按需申请测试，交付整体实施方案、单系统测试报告，报告提交时间测试完成后一周内。服务期内基于渗透测试成果，完成防控运营平台调优，实现成果管理和闭环。

1.2.3.29安全培训服务

完成面向省数字政府单位的网络及数据安全相关培训；内容不限于安全意识、安全管理、安全开发、安全加固；按需完成技术骨干人员集中培训，培训次数不少于1次，每次课时不少于6个；其余培训具体次数和课时不限；交付不限于培训视频、录制视频、培训资料、签到表、培训质量反馈表等。

1.2.3.30数据风险监测分析服务

完成采购人管理的统建通用系统的自有业务系统、数据公共支撑平台的7×24小时数据安全采集服务，对西咸联通主数据中心、西咸信创云数据中心、省信息化中心机房、新建高性能政务云等数据中心的数据库登录、操作、访问、风险、脆弱性风险、敏感数据访问等提供专项数据安全监测分析服务，完成5×8小时现场监测；风险的风险行为实时告警，协助完成处置，处置完成后的复测；对因客观原因无法完成处置的，提供必要措施控制风险并加强监控；交付不限于风险汇总表、月度、年度总结报告；需实时更新、实时提醒、汇总归档。

采购人提供服务所需的数据安全采集工具，工具为国产化设备且能支撑各采集区域的流量需求；至少满足监控区域≥10个，提供服务工具≥10台，每个区域工具监测流量能力≥10G，为国产化硬件工具产品，可存储审计日志天数≥180天，具备≥4个千兆电口、≥6个万兆光口，双冗余电源，提供符合要求的千兆、万兆接口及模块。

▲提供现有环境（云环境、物理网络环境）下的数据流量检测、加密流量解密监测审计、数据库性能分析、性能指标、趋势、历史对比、平均执行时长、次数等；提供多条件日志查询、敏感数据处理；提供数据库日志分析筛选，包含账号、IP、操作类型、数据库名/实例名等；提供数据安全风险检测能力，检测常见数据安全风险，可添加信任；提供含IP、端口、账号、操作类型、数据库名、表名等数据库访问路径展示；相关数据可导入协调指挥和防控运营平台；投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。服务期内，完成对接现网数据安全平台，与现网协调指挥平台实现数据资产、风险同步、管理以及数据安全建模分析。

1.2.3.31接口安全监测工具服务

完成采购人管理的统建通用系统的自有业务系统、数据公共支撑平台7×24小时接口安全监测服务，对信创云数据中心互联网区及政务外网区、信息中心互联网区及政务外网区的接口调用、访问、脆弱性风险、敏感数据流动等，提供专项接口安全监测分析服务，投标人提供满足采集要求的专业工具，审批后使用；提供5×8小时现场监测，针对风险行为提供预警，风险处置完成后，完成风险复测验证闭环，对因客观原因无法处置的风险，采取合理措施控制风险并加强监测，形成记录归档；以上采集、分析数据能够通过协调指挥和防控运营平台闭环管理。交付不限于风险汇总表、提醒单、月度、年度总结报告；需实时更新、实时提醒、汇总归档。服务期内，需实现与现网协调指挥平台的接口资产、风险同步、管理分析、展示等。

采购人提供服务所需的接口安全采集工具，工具为国产化设备且能支撑各采集区域的流量需求；至少满足监控区域≥10个，提供服务工具≥10台，每个区域工具监测流量能力≥8G，为国产化硬件工具产品，可存储审计日志天数≥180天，具备≥4个千兆电口、≥6个万兆光口，双冗余电源，提供符合要求的千兆、万兆接口及模块。

▲提供应用API结构、API访问量趋势、接口账号信息、传输文件展示，含应用、接口名称、接口URI、接口类型、接口敏感属性、API生命周期、返回类型、数据标签、端至应用访问关系图、传输文件次数及信息等采集；实现基于正则表达式、关键字等敏感数据识别，自定义请求头/响应头/请求体/响应体；识别访问次数、敏感数据、上传下载文件、登录账号数等行为监测；统计分析访问账号、应用、行为画像，关联风险原始日志；提供API接口风险详情信息，含风险基本信息、历史记录、API风险评估、修复建议、同类风险API对比等；提供接口访问日志

记录及详情信息；投标需提交工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

1.2.3.32数据安全管理服务

完成采购人指定或按需申请系统的数据安全风险评估服务，服务期内评估系统 ≥ 5 个，从技术和管理两方面开展评估，调研安全脆弱性、识别风险点、量化系统风险隐患、提出控制措施、输出评估报告；报告通过协调指挥与防控运营平台进行流转，形成风险告警和处置闭环管理，对处置后风险完成二次验证，服务期内指定的每系统完成至少1次。交付不限于评估方案、报告、过程资料文档。

1.2.3.33供应链安全评估服务

完成采购人指定核心重要业务系统的供应链安全风险评估服务，服务期内评估系统 ≥ 7 个，每重要系统供应链评估1次，报告通过协调指挥与防控运营平台进行流转，形成风险告警和处置闭环管理，对处置后风险完成二次验证。参考相关的国际标准、国内标准和行业的相关规范要求，对重要业务系统资产面临的供应链安全风险进行评估，完成供应链风险识别、分析和评价，识别供应链中安全风险、量化评估风险、潜在影响、协助改进管理控制措施，提供整体方案和评估报告。

1.2.3.34源代码安全审计服务

完成采购人指定或按需申请系统的源代码安全审计服务，服务期内评估系统 ≥ 20 个。提供专业的代码审计工具和代码组件成分评估工具，采用工具扫描和人工分析相结合的方式，对被测系统的开发语言、框架、代码漏洞、逻辑结构缺陷、代码缺陷、开源软件代码、组件等进行分析，审计内容包括但不限于输入验证、身份鉴别、授权管理、安全加密、错误处理、日志记录、逻辑结构分析等方面，开源组件识别内容包括但不限于软件成本名称、版本、已知漏洞等级、许可协议、漏洞利用难度等，并对软件依赖关系进行分析。发现源代码存在的安全漏洞和软件组件成分存在的已知安全漏洞，对软件组件漏洞及代码质量问题进行重点检查，兼容CNVD、CNNVD、Github等漏洞情报信息，覆盖常见的组件漏洞类型，对开源软件许可证进行分析，关联分析许可协议风险和许可依赖，出具整体实施方案、源代码审计报告和代码组件成分评估报告，并通过网络安全协调指挥及防控运营平台下发，提供修复建议协助开发人员修复安全问题，在业务方修复安全风险问题后，完成复测验证，确保安全风险问题完全修复。对因客观原因暂时无法修复的问题，给出安全建议，协助进行风险规避或降低，并记录。投标需提交使用工具的功能证明材料，不限产品截图、官网说明、第三方证明材料等。

1.2.4人员配置要求

投标人必须针对本项目组建专项技术服务团队，驻场服务人员不少于23人，其中驻场安全运营经理1人，驻场服务工具保障人员不少于1人，驻场平台保障人员不少于1人，驻场公共支撑日志平台保障人员不少于1人，驻场安全运营服务人员不少于19人。本项目所有人员需为投标人自有人员，不得分包、转包。服务人员上岗前需进行背景调查，确保安全后方可上岗。中标人须书面承诺，如在项目执行过程中发现服务团队不能胜任相关工作的，采购人有权要求更换，如中标人需主动调整服务团队成员，中标人须书面向采购人提出申请并取得采购人同意后方可调整。以上要求如有违反，则视为违约行为，采购人有权终止服务合同。

为保障网络安全运营工作有序开展，运营服务方需建立完善的安全运营组织。应根据实际服务需求，设置相应的服务岗位，安排合适的安全服务人员，每个岗位均须为安全运营服务方自有人员，以保证安全运营服务质量。

1.2.5设施设备配置要求

投标人按照服务响应时间需求、人员需求自行准备本地化服务所需的工具、设施、办公配套条件等。

投标人应提供本项目服务所需的所有必备工具、零配件、辅料辅材、办公设施等，工具应包括但不限于本项

目要求的工具类型、数量，工具符合国家和政府行业标准规范要求。本次服务的所提供的服务工具数据（包括但不限于系统运行产生的数据、图像及视频信息）的所有权归采购人所有，采购人获得本项目所有现场非可移动、非远程服务工具的服务期限内的使用和升级权利。本项目所有服务工具中的数据、服务产生的过程数据的所有权和使用权都属采购人，采购人对本项目中的全部数据资料具有独占性，未经采购人同意，投标人无权使用、转让或处理服务过程、成果数据。投标人不得保存和远程备份服务工具的数据，但应提供合适的技术手段，使之不被破坏、未经授权删除或盗取，并使采购人能合理使用、处理和备份服务相关数据。

在采购人现场工作的服务人员需随身佩戴工作证件，标明岗位、负责事务，遵守采购人的规章制度及工作守则，办公期间不从事与现场岗位无关的活动。服务人员未征得同意，不得使用相关用户的计算机，不得随意翻看用户办公资料物品；未经同意，不得拍摄、传播、留存用户相关数据信息；服务人员不得越权使用云网基础设施、系统、平台等的任何功能；不得私自拷贝用户业务系统中的任何数据和程序；所有重要操作行为均需进行报备方可进行，并对操作行为和结果进行记录。

项目服务期间应保障采购人现有网络系统、应用系统的正常运行，未经采购人允许不得擅自改动网络系统现状、业务系统配置，包括但不限于：网络架构和设备端口关系、设备IP配置、策略配置、系统参数、应用系统参数等。

1.3商务要求

1.3.1管理要求

投标人应在合同签订后14天内提交本项目总体进度控制计划，应至少包括项目执行各项服务的分阶段工作内容、服务工作计划开始与完成日期、完成每项工作所需的时间，报采购单位确认。

投标人应采取各种控制手段保证项目实施的各项服务按计划开始和结束。各阶段工作结束时，应结合工期、成本、质量评价项目进度状况，分析其中的问题，并提出下一阶段工作安排。

在合同开始执行后投标人应每周一次或在项目重大节点完成后以书面形式向网络安全管理咨询方及采购单位汇报计划的执行情况，对计划外的变更情况，应报监理方、采购单位同意后进行，并着重说明未能按计划开展或完成工作的原因，并采取措施制定完成及改进计划。

要求本项目服务内容和过程都能在协调指挥及防控运营平台上进行流转、汇总分析和集中展现。

1.3.2质量要求

投标人应严格按照质量体系的规定，制定项目质量控制措施，保证在项目执行的各个阶段均得到有效控制，所有质量控制过程均应有质量记录，以便进行服务全流程质量的追溯。

对于合同的各个阶段，投标人必须制订和执行质量保证监督计划，清楚地阐明对各个阶段的检查验收和测试方法，确保项目实施的各项内容都能满足国家标准和采购单位要求。

（1）项目全过程监理

本项目引入监理制，监理对本项目进行全过程的监督。投标人在项目组织和实施计划中应考虑到监理要求，实施过程中要积极配合监理工作，以保证项目实施的进度和质量。

（2）项目全过程监督

本项目引入第三方监督制，由网络安全管理监督服务单位对本项目运营服务单位进行全过程的监督。对技术运营服务单位进行监督、评价、审计，评价结果影响服务方的最终服务费用。投标人在项目组织和实施计划中应考虑到第三方监督要求，实施过程中要积极配合评价审计工作，以保证项目服务的质量。按照采购人和监督管理服务方制定的考核标准进行考核，考核结果应用于费用结算。

（3）文档管理

在项目实施过程中，由于项目实施的复杂性，双方人员参加以及时间跨度长等因素，所以有关过程文档都需

| | | |
|--|--|--|
| | | <p>文档化、标准化，以便查阅和引用。实施文档应作为项目成果的组成部分。</p> <p>项目文档至少应包括：项目管理文档、服务过程文档、服务团队提交并由采购人确认的相关文档、服务成果文档、采购人签署的阶段成果确认书、项目总结报告等。</p> <p>文档管理内容主要包括文档命名标准、文档的版本控制、文档的批准和存档，最终交付文档需满足档案管理要求。</p> <p>1.3.3交付标准</p> <p>投标人必须按照省级竣工验收管理办法要求进行交付验收，在签订合同前需明确交付验收资料清单和考核标准，并作为合同附录。</p> <p>投标人必须具备专业的安全服务能力和人员完成服务的交付，人员具备本项目要求相关的资历及资质证书。</p> <p>本项目所有服务成果交付需满足服务要求中各项服务的服务成果及交付标准，服务过程及执行技术标准满足网络安全管理监督服务单位制定的服务技术标准规范和考核评价要求，所有服务成果资料通过协调指挥及防控运营平台完成在线管理和流转。</p> <p>招标需求中的要求均为最低需求，投标人需根据实际服务需求，考虑增量和突发情况，根据实际完成全部服务要求，服务期内不增加任何费用。</p> <p>本项目需配合采购人完成公共支撑日志工具的等保三级、密评三级测评。</p> <p>1.3.4验收标准</p> <p>本项目验收前需通过省数据和政务服务局、省数据和政务服务中心、网络安全管理监督服务单位的联合考核，考核通过方可验收。考核内容范围为：所有服务项的完成指标工作量、响应及时性、服务质量、服务态度、文档交付等情况的综合考核。</p> <p>1.3.5成果归属</p> <p>1.中标人为履行本项目义务所形成的服务成果的知识产权归采购人所有。本项目不会引起任何已申请、登记的知识产权所有权的转移。</p> <p>2.本合同所涉及的所有数据的所有权归采购人所有。中标人只能用于履行本合同之义务。</p> <p>3.中标人提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权等方面的有关规定和要求。</p> <p>4.中标人保证向采购人提供的服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因中标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，中标人应负责解决并赔偿因此给采购人造成的全部损失。</p> <p>1.3.6保密要求</p> <p>中标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。中标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。中标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人内部与该项目无关的任何人员。</p> <p>1.4付款方式</p> |
|--|--|--|

3.2.3人员配置要求

付款条件说明：在合同签订生效后，达到付款条件起7日内，支付合同总金额的40.00%，交付验收合格后支

采购包1：

付合同剩余总金额60%。

▲服务人员要求。服务团队成员不少于8人；团队负责人1人，5年以上相关工作经验，具备高级工程师（信息化类）、信息系统项目管理师、咨询工程师证书；网络安全专业人员1人，10年以上网络安全相关工作经验，具备CISP证书(注册信息安全专业人员)、CCSC证书（网络与信息安全应急人员），网络安全高级工程师职业资格（工信认证）；项目专家人员2人，10年以上信息化咨询经验，具备人社评定的高级工程师（信息化类）；项目组成员4人，3年以上工作经验，具备咨询工程师证书。提供网络安全专业人员1人、专家人员2人，共3人的驻场工作，且实际服务人员不变更的承诺函。中标人须书面承诺，如在项目执行过程中服务团队不能胜任相关工作的，采购人有权要求更换，中标人自收到采购人的人员更换要求之日起两周内安排符合采购文件要求且能胜任相关工作的人员到场。如须调整服务团队成员，中标人须书面向采购人提出申请并取得采购人同意后调整。以上要求如有违反，则视为违约行为，采购人有权终止服务合同。

采购包2：

投标人必须针对本项目组建专项技术服务团队，驻场服务人员不少于23人，其中驻场安全运营经理1人，驻场服务工具保障人员不少于1人，驻场平台保障人员不少于1人，驻场公共支撑日志平台保障人员不少于1人，驻场安全运营服务人员不少于19人。本项目所有人员需为投标人自有人员，不得分包、转包。服务人员上岗前需进行背景调查，确保安全后方可上岗。中标人须书面承诺，如在项目执行过程中发现服务团队不能胜任相关工作的，采购人有权要求更换，如中标人需主动调整服务团队成员，中标人须书面向采购人提出申请并取得采购人同意后方可调整。以上要求如有违反，则视为违约行为，采购人有权终止服务合同。为保障网络安全运营工作有序开展，运营服务方需建立完善的安全运营组织。应根据实际服务需求，设置相应的服务岗位，安排合适的安全服务人员，每个岗位均须为安全运营服务方自有人员，以保证安全运营服务质量。

3.2.4设施设备配置要求

采购包1：

投标人按照服务响应时间需求、人员需求自行准备本地化服务所需的设施。▲投标人自行提供评价管理平台，平台系统满足云化和国产化部署要求，具备服务所需数据的接入能力、交付成果管理能力、管理过程数据展示能力等，并可按照采购人要求自定义指标库管理，指标库涵盖信息安全风险管理所需各类指标项内容，提供标准化指标项并可自定义管理指标项内容，通过指标选取、测量周期配置、指标值分制设置等，可自动计算指标得分；对于风险管理目标可实现同步性指标管理；提供运营分析能力，基于综合运营、质量分析、合规分析、人员分析、能力分析及自定分析得出安全管理指标数据；有效反应并管理网络安全运营服务、网络安全监督服务的服务进度及服务质量；服务开始时平台需直接投入适用，提供证明材料。采购人享有工具使用权和工具使用过程中产生的数据的所有权，未经采购人允许不得随意停止、撤换平台化工具。在采购人现场工作的投标人驻场服务人员，现场服务时需随身佩戴工作证件，标明岗位、负责事务，遵守局和中心的规章制度及工作守则，办公期间不从事与现场岗位无关的活动。服务人员未征得同意，不得使用相关用户的计算机，不得随意翻看用户办公资料物品；未经同意，不得拍摄、传播、留存用户相关数据信息；服务人员不得越权使用云网基础设施、系统、平台等的任何功能；不得私自拷贝用户业务系统中的任何数据和程序；所有重要操作行为均需进行报备方可进行，并对操作行为和结果进行记录。项目服务期间应保障采购人现有网络系统、应用系统的正常运行，未经采购人允许不得擅自改动网络系统现状、业务系统配置，包括但不限于：网络架构和设备端口关系、设备IP配置、策略配置、系统参数、应用系统参数等。

采购包2：

投标人按照服务响应时间需求、人员需求自行准备本地化服务所需的工具、设施、办公配套条件等。投标人应提供本项目服务所需的所有必备工具、零配件、辅料辅材、办公设施等，工具应包括但不限于本项目要求的工具类型、数量，工具符合国家和政府行业标准规范要求。本次服务的所提供的服务工具数据（包括但不限于系统运行产生的数据、图像及视频信息）的所有权归采购人所有，采购人获得本项目所有现场非可移动、非远程服务工具的服务期限内的使用和升级权利。本项目所有服务工具中的数据、服务产生的过程数据的所有权和使用权都属采购人，采购人对本项目中的全部数据资料具有独占性，未经采购人同意，投标人无权使用、转让或处理服务过程、成果数据。投标人不得保存和远程备份服务工具的数据，但应提供合适的技术手段，使之不被破坏、未经授权删除或盗取，并使采购人能合理使用、处理和备份服务相关数据。在采购人现场工作的

服务人员需随身佩戴工作证件，标明岗位、负责事务，遵守采购人的规章制度及工作守则，办公期间不从事与现场岗位无关的活动。服务人员未征得同意，不得使用相关用户的计算机，不得随意翻看用户办公资料物品；未经同意，不得拍摄、传播、留存用户相关数据信息；服务人员不得越权使用云网基础设施、系统、平台等的任何功能；不得私自拷贝用户业务系统中的任何数据和程序；所有重要操作行为均需进行报备方可进行，并对操作行为和结果进行记录。项目服务期间应保障采购人现有网络系统、应用系统的正常运行，未经采购人允许不得擅自改动网络系统现状、业务系统配置，包括但不限于：网络架构和设备端口关系、设备IP配置、策略配置、系统参数、应用系统参数等。

3.2.5其他要求

采购包1:

本项目不组织答疑会和现场考察，投标人可根据实际情况自行开展现场考察，投标人考察现场所发生的一切费用由投标人自行承担。

采购包2:

中标人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。中标人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。中标人在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人内部与该项目无关的任何人员。

3.3商务要求

3.3.1服务期限

采购包1:

自合同签订之日起七个月

采购包2:

自合同签订之日起七个月

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:

依招标文件和最终签订合同为准

采购包2:

依招标文件和最终签订合同为准

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: 在合同签订生效后，达到付款条件起 7 日内，支付合同总金额的 40.00%。

采购包1：付款条件说明： 交付验收合格后 ， 达到付款条件起 7 日内，支付合同总金额的 60.00%。

采购包2：付款条件说明： 在合同签订生效后 ， 达到付款条件起 7 日内，支付合同总金额的 40.00%。

采购包2：付款条件说明： 交付验收合格后 ， 达到付款条件起 7 日内，支付合同总金额的 60.00%。

3.3.6违约责任与争议解决的方法

采购包1：

依招标文件和最终签订合同为准

采购包2：

依招标文件和最终签订合同为准

3.5其他要求

无

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。 | 服务内容及服务邀请 应答表 投标函 商务应答表 投标文件封面 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 | 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。 | 服务内容及服务邀请 应答表 投标函 商务应答表 投标文件封面 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 | 资格审查要求概况 | 评审点具体描述 | 关联格式 |
|----|------------|--|---------------------|
| 1 | 本项目的特定资格要求 | <p>1、有效的主体资格证明：投标供应商为具有独立承担民事责任能力的法人或其他组织。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件； 2、法定代表人授权书/身份证明书：法定代表人直接参与投标的，须递交《法定代表人身份证明书》和身份证复印件。法定代表人授权代表参加投标的，须递交《法定代表人授权委托书》及授权代表身份证复印件； 3、财务状况：提供具有财务审计资质单位出具的完整2023年度的财务报告（成立时间至投标文件递交截止时间不足一年的可提供成立后任意时段的资产负债表）或投标文件递交截止时间前六个月内其开户银行出具的资信证明； 4、社会保障资金缴纳证明：供应商提供2024年至今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障参保缴费情况证明，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、税收缴纳证明：供应商提供2024年度至今至少一个月的纳税证明或完税证明，纳税证明或完税证明上应有代收机构或税务机关的公章，依法免税的供应商应提供相关文件证明； 6、专业技术能力的声明：提供具有履行本合同所必需的专业能力的声明。 7、无重大违法记录声明：供应商应具备良好的商业信誉，提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明； 8、信用记录查询结果：供应商应在投标截止日前，以“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）国家企业信用信息公示系统（https://www.gsxt.gov.cn/index.html）截图查询结果为准，提供（查询日期为从招标文件发售之日起至投标截止日前）网站截图并加盖供应商公章（开标当天代理机构现场查询，若不符合要求，按无效标处理），查询内容为未被列入失信被执行人、重大税收违法案件当事人</p> | 投标函 投标人应提交的相关资格证明材料 |

| | | | |
|--|--|--|--|
| | | 名单（处罚 期限届满的除外）和政府采购严重违法失信行为记录。 9、企业关联关系声明：单位负责人为同一人或者存在直接控股、管理关系的不同投标供应商，不得参加同一合同项下的政府采购活动； 注：本项目不接受联合体投标。 | |
|--|--|--|--|

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 | 本项目的特定资格要求 | <p>1、有效的主体资格证明：投标供应商为具有独立承担民事责任能力的法人或其他组织。企业法人应提供合法有效的标识有统一社会信用代码的营业执照；事业法人应提供事业单位法人证书；其他组织应提供合法登记证明文件； 2、法定代表人授权书/身份证明书：法定代表人直接参与投标的，须递交《法定代表人身份证明书》和身份证复印件。法定代表人授权代表参加投标的，须递交《法定代表人授权委托书》及授权代表身份证复印件； 3、财务状况：提供具有财务审计资质单位出具的完整2023年度的财务报告（成立时间至投标文件递交截止时间不足一年的可提供成立后任意时段的资产负债表）或投标文件递交截止时间前六个月内其开户银行出具的资信证明； 4、社会保障资金缴纳证明：供应商提供2024年至今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障参保缴费情况证明，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、税收缴纳证明：供应商提供2024年度至今至少一个月的纳税证明或完税证明，纳税证明或完税证明上应有代收机构或税务机关的公章，依法免税的供应商应提供相关文件证明； 6、专业技术能力的声明：提供具有履行本合同所必需的专业技术能力的声明。 7、无重大违法记录声明：供应商应具备良好的商业信誉，提供参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明； 8、信用记录查询结果：供应商应在投标截止日前，以“信用中国”网站（www.creditchina.gov.cn）和中国政府采购网（www.ccgp.gov.cn）国家企业信用信息公示系统（http://www.gsxt.gov.cn/index.html）截图查</p> | 投标函 投标人应提交的相关资格证明材料 |

| | | | |
|--|--|--|--|
| | | 询结果为准，提供（查询日期为从招标文件发售之日起至投标截止日前）网站截图并加盖供应商公章（开标当天代理机构现场查询，若不符合要求，按无效标处理），查询内容为未被列入失信被执行人、重大税收违法案件当事人名单（处罚 期限届满的除外）和政府采购严重违法失信行为记录。 9、企业关联关系声明：单位负责人为同一人或者存在直接控股、管理关系的不同投标供应商，不得参加同一合同项下的政府采购活动； 注：本项目不接受联合体投标。 | |
|--|--|--|--|

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 |
|----|----------------|----------------|-------------------------------|
| 1 | 本项目不专门面向中小企业采购 | 本项目不专门面向中小企业采购 | 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件 |

采购包2:

| 序号 | 资格审查要求概况 | 评审点具体描述 | 关联格式 |
|----|----------------|----------------|-------------------------------|
| 1 | 本项目不专门面向中小企业采购 | 本项目不专门面向中小企业采购 | 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 投标函 标的清单 |

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） | <p>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。</p> <p>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。</p> | 开标一览表 投标函 标的清单 |

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90.0000分 报价得分10.0000分 | | | |
| 评审因素分类 | 评审项 | 详细描述 | 分值 | 客观/主观 | 关联格式 |
| | 网络安全管理监督规范服务需求 | 结合国家和陕西省有关网络安全的标准、规范、制度等，充分理解网络安全管理要求，提出管理指标、评价指标和风险管理等有关建议，对建议的合理性和可操作性进行比较；满分6分。 1）内容合理，描述清晰，且能针对性满足项目需求的，得6分； 2）内容基本合理，描述简单，可行性一般，基本满足项目需要的，得4分； 3）内容笼统，描述简单，可行性较差，得2分； 4）未提供得0分。 | 6.0000 | 主观 | 商务应答表 服务方案 投标文件封面 投标函 |
| | | | | | |

| | | | | |
|------------|---|--------|----|------------------------------|
| 管理评价规范服务需求 | 结合陕西省数字政府有关管理制度，充分理解网络安全管理需求，提出的管理评价指标分类合理，具体内容具有参考性，并可通过平台进行数据分析；满分6分。1）内容合理，描述清晰，且能针对性满足项目需求的，得6分；2）内容基本合理，描述简单，可行性一般，基本满足项目需要的，得4分；3）内容笼统，描述简单，可行性较差，得2分；4）未提供得0分。 | 6.0000 | 主观 | 商务应答表 服务方案 |
| 运营评价服务 | 结合技术运营工作内容，提出运营评价方案，措施得当，评价效果清晰，可通过平台化工具管理合规审计管理；满分6分。1）内容合理，描述清晰，且能针对性满足项目需求的，得6分；2）内容基本合理，描述简单，可行性一般，基本满足项目需要的，得4分；3）内容笼统，描述简单，可行性较差，得2分；4）未提供得0分。 | 6.0000 | 主观 | 商务应答表 服务方案 售后服务承诺.docx |
| 合规审计服务 | 结合技术运营工作内容，提出合规审计措施得当，审计效果清晰，可通过平台化工具管理合规审计管理；满分6分。1）内容合理，描述清晰，且能针对性满足项目需求的，得6分；2）内容基本合理，描述简单，可行性一般，基本满足项目需要的，得4分；3）内容笼统，描述简单，可行性较差，得2分；4）未提供得0分。 | 6.0000 | 主观 | 商务应答表 服务方案 |

| | | | | | |
|------|----------|---|--------|----|---------------|
| 详细评审 | 平台化工具需求 | 充分理解平台化工具需求，提供与网络安全管理监督服务相关的各项指标要求、工具的证明材料和服务交付管理方案的情况下，视响应情况得分；满分9分。1）内容完整、描述清晰，提供自定义指标库、同步管理、安全运营指标管理，能够提供详细方案设计，能针对性满足项目需求并为成品工具，得9分；2）内容完整，描述较清晰，能满足项目需要，能在服务开始前交付，得7分；3）内容基本完整，描述简单，基本满足项目需要，能在服务开始时交付，得5分；4）内容笼统，描述简单，可行性较差，能在服务开始后1个月内交付，得3分；5）未提供得0分。 | 9.0000 | 主观 | 商务应答表 服务方案 |
| | 安全风险管理需求 | 按照安全风险进行总体设计，合理利用专家咨询和风险会商机制，保证咨询服务的顺利开展；满分5分。1）提供了详细的框架设计并与服务中各项内容进行高度融合管理的，得5分；2）提供了一般框架设计，与服务各项内容有对应关系的，得3分；3）内容笼统，描述简单，无对照关联的，得1分；4）未提供得0分。 | 5.0000 | 主观 | 商务应答表 服务方案 |
| | 项目质量管理 | 对本项目的质量保证措施要求；满分5分。1）质量保证安排针对性强，计划安排具体，质量保证措施全面可行，得5分；2）质量保证满足基本要求，计划安排较合理，质量保证措施可行，得3分；3）内容笼统，描述简单，无对照关系，得1分；4）未提供得0分。 | 5.0000 | 主观 | 商务应答表 服务方案 |
| | | | | | |

| | | | | |
|-------|---|--------|----|---------------|
| 合理化建议 | 提供省数字政府网络安全监测提升及服务优化项目及省数字政务网络安全的合理化建议和规划；满分5分。1）能够提供有针对性且全面的合理化建议，有效促进网络安全监测提升及服务优化项目高质量开展、促进数字政务安全发展的，得5分；2）能够提供一定得合理化建议服务于网络安全监测提升及服务优化项目的，得3分；3）能够提供具备参考价值建议的，得1分；4）未提供得0分。 | 5.0000 | 主观 | 商务应答表 服务方案 |
| 履约能力 | 投标人能够熟悉并了解数字政务系统现状，并能够深刻分析识别当前面临的问题，结合网络安全监测提升及服务优化项目提出有效措施保障服务质量，满分5分。1）对数字政务背景和现状熟悉、能够深刻分析识别当前面临的问题，清晰描述建议措施的，得5分；2）对数字政务背景和现状了解，能分析识别部分问题，得3分；3）未提供得0分。 | 5.0000 | 主观 | 商务应答表 服务方案 |
| 履约能力 | 要求中的▲号为关键指标项，投标人需每项如实响应，全部满足得5分，一项不满足扣1分，扣完为止。 | 5.0000 | 客观 | 商务应答表 服务方案 |

| | | | | |
|------|--|---------|----|-----------------------------|
| 履约能力 | 项目服务实施保障的合理性和可操作性进行比较。服务团队人员不少于8人；满分18分。1）项目负责人1人，同时具备高级工程师（信息化类）、信息系统项目管理师、咨询工程师证书得6分，缺少1项扣2分，扣完为止。2）项目网络安全专业人员1人，应具备CISP证书(注册信息安全专业人员),CCSC证书（网络与信息安全应急人员），网络安全高级工程师职业资格（工信认证），并提供同类项目履历和人员驻场承诺，以上要求均具备得4分，缺少1项扣2分，扣完为止。3）项目专家人员2人，应具备人社评定的高级工程师（信息化类）并提供同类项目履历，并提供人员驻场承诺；以上要求均具备1人得2分，共4分，缺少1项扣2分，扣完为止。4）项目组成员4人，应具备咨询工程师证书并提供基本履历，1人得1分，共4分，缺少1项扣1分，扣完为止。以上人员必须同时出具该工程师在本单位的近6个月内任意1个月的社保缴纳证明材料。 | 18.0000 | 客观 | 商务应答表 服务方案 驻场承诺书.docx |
| 履约能力 | 本次项目生成的安全保障体系规范应结构完整，符合国家安全标准，符合等级保护管理要求，并具备可落地的执行能力。需提供证明文件复印件并加盖公章；满分8分。1）信息安全服务资质认证证书，得2分，不提供得0分。2）数据管理能力成熟度评估认证证书，得2分，不提供得0分。3）ISO90001质量体系认证，得2分，不提供得0分。4）工程咨询单位【电子、信息工程（含通信、广电、信息化）】备案证明得2分，未提供得0分。 | 8.0000 | 客观 | 商务应答表 服务方案 其他资料.docx |

| | | | | | |
|-----|------|---|----------------|----|------------------------------------|
| | 履约能力 | 提供 2022年1月1日 至今同类业绩的合同证明材料，以响应文件中合同复印件为计分依据，提供合同关键页（包括但不限于合同首页、服务内容页、合同金额页、合同盖章页）复印件；每提供 1个 得 2分 ，最高得 6分 。 | 6.0000 | 客观 | 商务应答表 服务方案 供应商类似项目业绩一览表.docx |
| 价格分 | 价格分 | 1. 经初审合格的投标响应文件，其投标报价为有效投标报价，并进行价格评审。 2. 满足文件要求且价格最低的报价为基准价，其价格分为满分 10分 。 3. 报价得分=（基准价/报价）× 10 的公式计算得分，计算分数时四舍五入取小数点后两位。 4. 明显低于成本价进行报价的投标视为无效投标。 | 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 | 10.0000% | 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90.0000分 报价得分10.0000分 | | | |
| 评审因素分类 | 评审项 | 详细描述 | 分值 | 客观/主观 | 关联格式 |

| | | | | | |
|--|--------|--|---------|----|---------------|
| | 服务需求理解 | 投标人需基于对省数字政府整体安全运营项目背景、现状、目标以及服务需求的描述进行需求理解，需理解透彻、描述详细、符合省数字政府安全现状和服务需求。 1.需求理解准确，描述详细合理，完全符合省数字政府安全现状和服务需求的，得12分； 2.整体理解合理，描述合理，基本符合省数字政府安全现状和服务需求的，得9分； 3.整体理解较为合理，描述清楚，符合逻辑，得6分； 4.理解有偏差，缺乏针对性，得3分； 5.未提供得0分。 | 12.0000 | 主观 | 商务应答表 服务方案 |
| | | | | | |

| | | | | |
|------|---|---------|----|---------------|
| 服务方案 | <p>投标人应基于对省数字政府整体安全运营需求的理解，编写整体安全运营服务方案，服务设计及交付符合省数字政府实际需求。从方案成熟度、完整性、符合程度等情况进行综合评分。</p> <p>1.投标人对服务内容中的安全监测提升服务、政务云安全监测引擎服务、公共支撑日志采集服务、公共支撑日志审计服务、平台设备扩容服务（5项服务）按服务要求逐项响应，各项服务方案架构设计合理、完整、描述得当，完全符合服务要求，单项服务方案得2分； 各项服务方案架构设计一般、但内容完整，基本符合服务要求，单项服务方案得1.5分； 方案架构设计一般、描述不当、不完全符合服务要求，单项服务方案得1分； 方案设计不周全，或其它，单项服务方案得0.5分； 未提供得0分。</p> <p>2.投标人对其它服务项进行响应，服务方案设计完整，单项服务响应至少包含服务目标、服务内容、服务交付清单及成果内容、服务频次、服务交付流程，服务方案设计完整、需求符合程度高、成熟度高的得10分； 服务设计完整、需求符合程度一般、成熟度一般的得6分； 服务设计不周全或其它得3分； 未提供得0分。</p> <p>3.投标人对整体服务组织、人员安排、服务工具实施设计合理，且服务交付方式符合省数字政府实际，利于按时交付。整体实施方案设计合理、符合现状需求，得5分； 设计较为合理、基本符合需求，得3分； 未提供得0分。</p> | 25.0000 | 主观 | 商务应答表 服务方案 |
|------|---|---------|----|---------------|

| | | | | | |
|------|--------|---|---------|----|------------------------------|
| 详细评审 | 服务要求响应 | <p>1.投标人对服务内容需求中的▲号内容逐条进行响应，全部满足得10分，一项不满足扣1分，扣完为止。</p> <p>2.本次项目所提供的威胁监测系统工具、漏洞扫描系统工具、全流量采集工具、攻击样本采集系统工具、专业镜像分流工具、非结构化数据监测工具（6类工具，满分6分），应完全满足服务要求，每按要求提供一项服务工具功能能力证明材料，且完全满足服务工具能力要求的得1分；能力证明材料不完全满足工具能力要求的，每提供一项得0.5分；未提供得0分。</p> <p>3.投标人对所有服务项中，需基于现场服务需求、成果、问题等调优的11项平台能力优化要求，提供设计说明响应，包括但不限于文字描述、图表描述、demo设计等方面，提供的响应内容设计合理、完全符合服务需求，每项得0.5分，最高满分5分；响应内容设计一般，基本符合服务需求，每项得0.2分；未提供得0分。</p> | 21.0000 | 主观 | 商务应答表 服务方案 其他资料.docx |
| | 质量保障 | <p>1.投标人需提供质量保障方案，至少包括健全的质量控制体系、针对本项目的质量把控方案、质量保障措施等。能够有效的保障项目实施过程、完善保证项目整体质量，提供对应措施，得5分；能够基本有效的保障项目实施过程、基本保证项目整体质量，提供对应措施，得3分；无法完全保障项目实施过程、无法完全保证项目整体质量，得1分；未提供得0分。</p> <p>2.根据项目服务中的优化内容要求，整理提供项目平台优化承诺函，得1分，未提供得0分。</p> <p>3.根据项目服务内容要求，整理提供项目交付承诺函，得1分；</p> <p>4.未提供得0分。</p> | 7.0000 | 主观 | 商务应答表 服务方案 售后服务承诺.docx |

| | | | | |
|---------|---|--------|----|---------------|
| 投标人能力证明 | <p>投标人具有有效期内的资质，按照资质情况得分。1.具备国家权威机构中国信息安全测评中心颁发的信息安全服务资质-安全工程类资质，三级计1分，其他级别计0.5分，未提供得0分；2.具备国家权威机构中国信息安全测评中心颁发的信息安全服务资质-风险评估类最高级别计1分，其他级别计0.5分，未提供得0分；3.具备国家权威机构中国信息安全测评中心颁发的信息安全服务资质-安全运营类，最高级别计1分，其他级别计0.5分，未提供得0分；4.具备国家权威机构中国信息安全测评中心颁发的信息安全服务资质-数据安全类，具有证书计1分，没有不计分，未提供得0分；5.针对重要数据保护需求，提供ISO/IEC 27701:2019隐私信息管理体系认证、ISO28000供应链安全管理体系认证证书，每个证书计1分，共2分，未提供得0分。</p> | 6.0000 | 客观 | 商务应答表 服务方案 |
| 项目经理 | <p>投标人拟投入本项目的项目经理（1名），具备有效期内以下资质： （1）本科学历及以上；（2）具备计算机技术与软件专业技术资格信息安全工程师；（3）具备注册信息安全工程师CISP证书；（4）具备注册数据安全治理CISP-DSG资质证书；（5）具备云安全工程师CISP-CSE资质证书；（6）具备注册渗透测试工程师CISP-PTE或注册渗透测试专家CISP-PTS证书；（7）具备信息安全保障人员应急服务证书。提供人员的学历证书、认证证书。总分5分，少提供1个扣1分。</p> | 5.0000 | 客观 | 商务应答表 服务方案 |

| | | | | |
|--------|--|--------|----|------------------------------------|
| 服务人员要求 | <p>投标人拟投入本项目服务工程师具备有效期内如下资质：项目所提供人员中应至少有4名工程师同时具备CISP、渗透测试相关证书；3名人员同时具备CISP、CISP-DSG数据治理相关证书；3名人员同时具备CISP、安全运维相关证书；3名人员同时具备CISP、应急响应相关证书；2名人员同时具备CISP、项目管理相关证书；2名人员同时具备CISP、信息安全工程师证书；3名人员同时具备CISP、CISP-CSE云安全证书。提供以上人员的认证证书，人员不得复用。提供简历及证书的且符合条件的全部满足的，满分6分，每少提供一个扣0.5分，扣完为止。</p> | 6.0000 | 客观 | 商务应答表 服务方案 驻场承诺书.docx |
| 培训师要求 | <p>培训师具备专业安全培训能力，具备以下有效期内资质：（1）硕士学历及以上；（2）计算机技术与软件专业技术资格高级证书；（3）具备注册安全讲师；（4）具备CISP-CSE云安全工程师；（5）具备注册信息安全工程师CISP证书；（6）具备安全运维相关证书。提供以上人员的学历证书、认证证书，提供人员在投标截止之日前六个月内任意一个月社保缴纳证明材料。总分3分，少提供一个扣0.5分。</p> | 3.0000 | 客观 | 商务应答表 服务方案 |
| 类似项目经验 | <p>投标人2022年1月1日至今（以合同签订时间为准）承担的同类项目案例，每提供一个符合要求的项目案例得1分，最高得5分。注：提供合同关键页（包括但不限于合同首页、服务内容页、合同金额页、合同盖章页）复印件，否则不得分。</p> | 5.0000 | 客观 | 商务应答表 服务方案 供应商类似项目业绩一览表.docx |

| | | | | | |
|-----|-----|--|---------|----|---------------|
| 价格分 | 价格分 | 1.经初审合格的投标响应文件，其投标报价为有效投标报价，并进行价格评审。2.满足文件要求且价格最低的报价为基准价，其价格分为满分10分。3.报价得分=（基准价/报价）×10的公式计算得分，计算分数时四舍五入取小数点后两位。4.明显低于成本价进行报价的投标视为无效投标。 | 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 | 10.0000 % | 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 |

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: 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: 服务内容及服务邀请应答表

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: 供应商类似项目业绩一览表.docx

详见附件: 售后服务承诺.docx

详见附件: 驻场承诺书.docx

详见附件: 其他资料.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: 服务内容及服务邀请应答表

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: 供应商类似项目业绩一览表.docx

详见附件: 驻场承诺书.docx

详见附件: 售后服务承诺.docx

详见附件: 其他资料.docx

第7章 拟签订采购合同文本

详见附件：合同.docx

