

招 标 文 件

(服务类)

采购项目名称：**2025年度陕西省数字政府网络安全管理运营服务项目**

采购项目编号：**HCXM-GK-2511-01**

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12月11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2025年度陕西省数字政府网络安全管理运营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：**HCXM-GK-2511-01**

二、采购项目名称：**2025年度陕西省数字政府网络安全管理运营服务项目**

三、招标项目简介

为全面筑牢省级数字政府安全屏障，我省已构建形成“政府主导、专业协同、权责清晰、监管有效”的一体化网络安全运营体系。采购人建设的“省数字政府网络安全协调指挥及防控运营平台”已成为安全运营的核心支撑平台，实现了对政务外网（广域网、接入区、省级城域网）、各省级政务云（含政法云）和核心应用系统等的安全监测管理，并可对接各类安全监测数据集中分析与响应处置管理。为进一步提升整体安全防护能力，本项目拟通过专项采购，围绕以下四大方向推进能力升级：一是拓展监测广度，实现省级政务云机房及云上业务的全面覆盖，构建全域感知、精准溯源的风险监测体系；二是强化数据赋能，依托统一日志审计平台，集约化提供全景日志服务，增强安全数据分析与利用能力；三是聚焦新兴风险，专项开展政务大模型安全评估与监测，引入专业化安全运营服务，应对新型技术场景下的安全挑战。四是通过专业的安全运营及咨询服务，提升省级数字政府网络安全管理运营能力。通过上述举措，最终实现网络安全风险的“可监测、可预警、可处置、可追溯”，达成“可视、可管、可控”的闭环管理目标。

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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）

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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）。

采购包3:

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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）。

采购包4:

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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）。

采购包5：

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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）。

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）	本项目各包采购预算金额如下： 采购包1：1,188,400.00元 采购包2：10,215,500.00元 采购包3：445,600.00元 采购包4：712,500.00元 采购包5：1,666,600.00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 采购包3：综合评分法 采购包4：综合评分法 采购包5：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 采购包3：不接受 采购包4：不接受 采购包5：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）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。 （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。 （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。

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：20,000.00元</p> <p>采购包2保证金金额：70,000.00元</p> <p>采购包3保证金金额：8,000.00元</p> <p>采购包4保证金金额：10,000.00元</p> <p>采购包5保证金金额：30,000.00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：6105 0192 5700 0000 0294</p>
10	标书费信息	免费获取
		<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%</p> <p>说明：1.履约保证金的性质与目的 1.1履约保证金是中标（成交）供应商（以下简称“供应商”）为保证其严格按照政府采购合同（以下简称“合同”）约定全面、诚信履行合同义务，向采购人提供的担保。 1.2履约保证金旨在督促供应商按期、按质、按量完成合同标的，并在其发生违约行为时，作为对采购人损失的一种补偿保障。 2.缴纳金额与形式 2.1履约保证金的金额为合同总金额的5%。 2.2供应商应以以下一种形式提交履约保证金： 电汇/转账：以现金形式汇入采购人指定的专用账户。 银行保函：由中华人民共和国境内注册的商业银行出具的不可撤销、见索即付保函，格式须经采购人认可，有效期应覆盖合同约定的全部履约期限及质量保证期。 保证保险：由具备相应资质的保险公司出具的履约保证保险保单，保险责任与金额须等同于现金保证。 2.3采用银行保函或保证保险形式的，其正本原件应在签订合同前提交给采购人。采用电汇形式的，应在合同签订后15个工作日内完成支付。 3.提交与生效条件 3.1履约保证金是合同生效的前提条件之一。供应商必须在与采购人签订合同前或合同约定的时间内完成提交。 3.2若供应商未按本要求及合同约定提交足额、有效的履约保证金，视为其放弃中标（成交）资格，采购人有权不予签订合同，并可按照相关法律法规及采购文件规定追究其责任。 4.使用与扣划 4.1在合同履行期间，如供应商出现下列违约情形之一，采购人有权根据合同约定及违约严重程度，部分或全部扣划履约保证金，且不排除供应商的合同责任： 1.未按合同约定的时间、地点、质量标准交付货物、完成工程或提供服务； 2.交付的货物、工程或服务不符合合同要求，经采购人提出后未在合理期限内纠正、更换或采取有效补救措施； 3.擅自将合同分包、转包； 4.因供应商原因导致合同无法继续履行或解除； 5.其他违反合同约定或法律法规的行为，给采购人造成损失。 4.2扣划履约保证金后，若不足以弥补采购人损失的，采购人有权依法向供应商进行追偿。 5.退还 5.1在供应商完全、适当地履行了合同全部义务（包括但不限于交货、安装、调试、验收合格、质量保证期届满等）后，履约保证金将予以无息退还。 5.2退还程序： 1.采用现金形式的，供应商应向采购人提出书面退还申请。采购人在收到申请并确认合同履行无误后15个工作日内，办理无息退还手续。 2.采用银行保函或保证保险形式的，该保函或保单在有效期届满后自动失效。采购人应在合同义务完全履行后，将保函或保单正本退还供应商。 5.3若合同履行过程中根据约定需变更履约保证金的，双方应签订补充协议。 6.其他 6.1履约保证金的有效期应持续至合同约定的项目最终验收合格之日。 6.2本项目不接受个人支票、现金或商业汇票作为履约保证金。 6.3履约保证金的提交、使用、退还等事宜，如本要求未详尽约定，以双方签订的政府采购合同相关内容为准。若发生争议，按合同争议解决条款执行</p>

采购包2：缴纳

本采购包履约保证金为合同金额的5%

说明：1.履约保证金的性质与目的 1.1履约保证金是中标（成交）供应商（以下简称“供应商”）为保证其严格按照政府采购合同（以下简称“合同”）约定全面、诚信履行合同义务，向采购人提供的担保。 1.2履约保证金旨在督促供应商按期、按质、按量完成合同标的，并在其发生违约行为时，作为对采购人损失的一种补偿保障。 2.缴纳金额与形式 2.1履约保证金的金额为合同总金额的5%。 2.2供应商应以以下一种形式提交履约保证金：电汇/转账：以现金形式汇入采购人指定的专用账户。银行保函：由中华人民共和国境内注册的商业银行出具的不可撤销、见索即付保函，格式须经采购人认可，有效期应覆盖合同约定的全部履约期限及质量保证期。保证保险：由具备相应资质的保险公司出具的履约保证保险保单，保险责任与金额须等同于现金保证。 2.3采用银行保函或保证保险形式的，其正本原件应在签订合同前提交给采购人。采用电汇形式的，应在合同签订后15个工作日内完成支付。 3.提交与生效条件 3.1履约保证金是合同生效的前提条件之一。供应商必须在与采购人签订合同前或合同约定的时间内完成提交。 3.2若供应商未按本要求及合同约定提交足额、有效的履约保证金，视为其放弃中标（成交）资格，采购人有权不予签订合同，并可按照相关法律法规及采购文件规定追究其责任。 4.使用与扣划 4.1在合同履行期间，如供应商出现下列违约情形之一，采购人有权根据合同约定及违约严重程度，部分或全部扣划履约保证金，且不排除供应商的合同责任： 1.未按合同约定的时间、地点、质量标准交付货物、完成工程或提供服务； 2.交付的货物、工程或服务不符合合同要求，经采购人提出后未在合理期限内纠正、更换或采取有效补救措施； 3.擅自将合同分包、转包； 4.因供应商原因导致合同无法继续履行或解除； 5.其他违反合同约定或法律法规的行为，给采购人造成损失。 4.2扣划履约保证金后，若不足以弥补采购人损失的，采购人有权依法向供应商进行追偿。 5.退还 5.1在供应商完全、适当地履行了合同全部义务（包括但不限于交货、安装、调试、验收合格、质量保证期届满等）后，履约保证金将予以无息退还。 5.2退还程序： 1.采用现金形式的，供应商应向采购人提出书面退还申请。采购人在收到申请并确认合同履行无误后15个工作日内，办理无息退还手续。 2.采用银行保函或保证保险形式的，该保函或保单在有效期届满后自动失效。采购人应在合同义务完全履行后，将保函或保单正本退还供应商。 5.3若合同履行过程中根据约定需变更履约保证金的，双方应签订补充协议。 6.其他 6.1履约保证金的有效期应持续至合同约定的项目最终验收合格之日。 6.2本项目不接受个人支票、现金或商业汇票作为履约保证金。 6.3履约保证金的提交、使用、退还等事宜，如本要求未详尽约定，以双方签订的政府采购合同相关内容为准。若发生争议，按合同争议解决条款执行

采购包3：缴纳

本采购包履约保证金为合同金额的5%

说明：1.履约保证金的性质与目的 1.1履约保证金是中标（成交）供应商（以下简称“供应商”）为保证其严格按照政府采购合同（以下简称“合同”）约定全面、诚信履行合同义务，向采购人提供的担保。 1.2履约保证金旨在督促供应商按期、按质、按量完成合同标的，并在其发生违约行为时，作为对采购人损失的一种补偿保障。 2.缴纳金额与形式 2.1履约保证金的金额为合同总金额的5%。 2.2供应商应以以下一种形式提交履约保证金：电汇/转账：以现金形式汇入采购人指定的专用账户。银行保函：由中华人民共和国境内注册的商业银行出具的不可撤销、见索即付保函，格式须经采购人认可，有效期应覆盖合同约定的全部履约期限及质量保证期。保证保险：由具备相应资质的保险公司出具的履约保证保险保单，保险责任与金额须等同于现

履约保证金（实质性要求）

金保证。2.3采用银行保函或保证保险形式的，其正本原件应在签订合同前提交给采购人。采用电汇形式的，应在合同签订后15个工作日内完成支付。3.提交与生效条件3.1履约保证金是合同生效的前提条件之一。供应商必须在与采购人签订合同前或合同约定的时间内完成提交。3.2若供应商未按本要求及合同约定提交足额、有效的履约保证金，视为其放弃中标（成交）资格，采购人有权不予签订合同，并可按照相关法律法规及采购文件规定追究其责任。4.使用与扣划4.1在合同履行期间，如供应商出现下列违约情形之一，采购人有权根据合同约定及违约严重程度，部分或全部扣划履约保证金，且不免除供应商的合同责任：1.未按合同约定的时间、地点、质量标准交付货物、完成工程或提供服务；2.交付的货物、工程或服务不符合合同要求，经采购人提出后未在合理期限内纠正、更换或采取有效补救措施；3.擅自将合同分包、转包；4.因供应商原因导致合同无法继续履行或解除；5.其他违反合同约定或法律法规的行为，给采购人造成损失。4.2扣划履约保证金后，若不足以弥补采购人损失的，采购人有权依法向供应商进行追偿。5.退还5.1在供应商完全、适当地履行了合同全部义务（包括但不限于交货、安装、调试、验收合格、质量保证期届满等）后，履约保证金将予以无息退还。5.2退还程序：1.采用现金形式的，供应商应向采购人提出书面退还申请。采购人在收到申请并确认合同履行无误后15个工作日内，办理无息退还手续。2.采用银行保函或保证保险形式的，该保函或保单在有效期届满后自动失效。采购人应在合同义务完全履行后，将保函或保单正本退还供应商。5.3若合同履行过程中根据约定需变更履约保证金的，双方应签订补充协议。6.其他6.1履约保证金的有效期应持续至合同约定的项目最终验收合格之日。6.2本项目不接受个人支票、现金或商业汇票作为履约保证金。6.3履约保证金的提交、使用、退还等事宜，如本要求未详尽约定，以双方签订的政府采购合同相关内容为准。若发生争议，按合同争议解决条款执行

采购包4：缴纳

本采购包履约保证金为合同金额的5%

说明：1.履约保证金的性质与目的1.1履约保证金是中标（成交）供应商（以下简称“供应商”）为保证其严格按照政府采购合同（以下简称“合同”）约定全面、诚信履行合同义务，向采购人提供的担保。1.2履约保证金旨在督促供应商按期、按质、按量完成合同标的，并在其发生违约行为时，作为对采购人损失的一种补偿保障。2.缴纳金额与形式2.1履约保证金的金额为合同总金额的5%。2.2供应商应以以下一种形式提交履约保证金：电汇/转账：以现金形式汇入采购人指定的专用账户。银行保函：由中华人民共和国境内注册的商业银行出具的不可撤销、见索即付保函，格式须经采购人认可，有效期应覆盖合同约定的全部履约期限及质量保证期。保证保险：由具备相应资质的保险公司出具的履约保证保险保单，保险责任与金额须等同于现金保证。2.3采用银行保函或保证保险形式的，其正本原件应在签订合同前提交给采购人。采用电汇形式的，应在合同签订后15个工作日内完成支付。3.提交与生效条件3.1履约保证金是合同生效的前提条件之一。供应商必须在与采购人签订合同前或合同约定的时间内完成提交。3.2若供应商未按本要求及合同约定提交足额、有效的履约保证金，视为其放弃中标（成交）资格，采购人有权不予签订合同，并可按照相关法律法规及采购文件规定追究其责任。4.使用与扣划4.1在合同履行期间，如供应商出现下列违约情形之一，采购人有权根据合同约定及违约严重程度，部分或全部扣划履约保证金，且不免除供应商的合同责任：1.未按合同约定的时间、地点、质量标准交付货物、完成工程或提供服务；2.交付的货物、工程或服务不符合合同要求，经采购人提出后未在合理期限内纠正、更换或采取有效补救措施；3.擅自将合同分包、转包；4.因供应商原因导致合同无法继续履行或解除；5.其他违反合同约定或法律法规的行为，给采购人造成损失。4.2扣划履约保证金后，若不足以弥补采购人损失的，采购人有权依法向

供应商进行追偿。 5.退还 5.1在供应商完全、适当地履行了合同全部义务（包括但不限于交货、安装、调试、验收合格、质量保证期届满等）后，履约保证金将予以无息退还。 5.2退还程序： 1.采用现金形式的，供应商应向采购人提出书面退还申请。采购人在收到申请并确认合同履行无误后15个工作日内，办理无息退还手续。 2.采用银行保函或保证保险形式的，该保函或保单在有效期届满后自动失效。采购人应在合同义务完全履行后，将保函或保单正本退还供应商。 5.3若合同履行过程中根据约定需变更履约保证金的，双方应签订补充协议。 6.其他 6.1履约保证金的有效期应持续至合同约定的项目最终验收合格之日。 6.2本项目不接受个人支票、现金或商业汇票作为履约保证金。 6.3履约保证金的提交、使用、退还等事宜，如本要求未详尽约定，以双方签订的政府采购合同相关内容为准。若发生争议，按合同争议解决条款执行

采购包5：缴纳

本采购包履约保证金为合同金额的5%

说明： 1.履约保证金的性质与目的 1.1履约保证金是中标（成交）供应商（以下简称“供应商”）为保证其严格按照政府采购合同（以下简称“合同”）约定全面、诚信履行合同义务，向采购人提供的担保。 1.2履约保证金旨在督促供应商按期、按质、按量完成合同标的，并在其发生违约行为时，作为对采购人损失的一种补偿保障。 2.缴纳金额与形式 2.1履约保证金的金额为合同总金额的5%。 2.2供应商应以以下一种形式提交履约保证金： 电汇/转账：以现金形式汇入采购人指定的专用账户。 银行保函：由中华人民共和国境内注册的商业银行出具的不可撤销、见索即付保函，格式须经采购人认可，有效期应覆盖合同约定的全部履约期限及质量保证期。 保证保险：由具备相应资质的保险公司出具的履约保证保险保单，保险责任与金额须等同于现金保证。 2.3采用银行保函或保证保险形式的，其正本原件应在签订合同前提交给采购人。采用电汇形式的，应在合同签订后15个工作日内完成支付。 3.提交与生效条件 3.1履约保证金是合同生效的前提条件之一。供应商必须在与采购人签订合同前或合同约定的时间内完成提交。 3.2若供应商未按本要求及合同约定提交足额、有效的履约保证金，视为其放弃中标（成交）资格，采购人有权不予签订合同，并可按照相关法律法规及采购文件规定追究其责任。 4.使用与扣划 4.1在合同履行期间，如供应商出现下列违约情形之一，采购人有权根据合同约定及违约严重程度，部分或全部扣划履约保证金，且不免除供应商的合同责任： 1.未按合同约定的时间、地点、质量标准交付货物、完成工程或提供服务； 2.交付的货物、工程或服务不符合合同要求，经采购人提出后未在合理期限内纠正、更换或采取有效补救措施； 3.擅自将合同分包、转包； 4.因供应商原因导致合同无法继续履行或解除； 5.其他违反合同约定或法律法规的行为，给采购人造成损失。 4.2扣划履约保证金后，若不足以弥补采购人损失的，采购人有权依法向供应商进行追偿。 5.退还 5.1在供应商完全、适当地履行了合同全部义务（包括但不限于交货、安装、调试、验收合格、质量保证期届满等）后，履约保证金将予以无息退还。 5.2退还程序： 1.采用现金形式的，供应商应向采购人提出书面退还申请。采购人在收到申请并确认合同履行无误后15个工作日内，办理无息退还手续。 2.采用银行保函或保证保险形式的，该保函或保单在有效期届满后自动失效。采购人应在合同义务完全履行后，将保函或保单正本退还供应商。 5.3若合同履行过程中根据约定需变更履约保证金的，双方应签订补充协议。 6.其他 6.1履约保证金的有效期应持续至合同约定的项目最终验收合格之日。 6.2本项目不接受个人支票、现金或商业汇票作为履约保证金。 6.3履约保证金的提交、使用、退还等事宜，如本要求未详尽约定，以双方签订的政府采购合同相关内容为准。若发生争议，按合同争议解决条款执行

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《招标代理服务收费管理暂行办法》（计价格【2002】1980号）及《国家发展改革委办公厅关于招标代理服务收费有关问题的通知》【2003】857号文件规定的收费标准，采购人向汇成项目管理有限公司交纳招标代理服务费。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> <p>采购包3：组织现场踏勘：否</p> <p>采购包4：组织现场踏勘：否</p> <p>采购包5：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、推荐中标候选供应商等活动。

2.3 招标文件

2.3.1 招标文件的构成

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

- （一）投标邀请；
- （二）投标人须知；
- （三）招标项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）评标办法；
- （六）投标文件格式；
- （七）拟签订采购合同文本。

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

2.3.2 招标文件的澄清和修改

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

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，投标人应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响投标文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4 投标文件

2.4.1 投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，评标委员会将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对投标人的不利后果，由投标人承担。

2.4.2 计量单位

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3 投标货币

本次项目均以人民币报价。

2.4.4 知识产权

一、投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

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

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

2.4.5 投标文件的组成

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

投标文件具体内容详见第六章。

2.4.6 投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7 投标报价（实质性要求）

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

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

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

2.4.8 投标有效期（实质性要求）

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

2.4.9 投标文件的制作、签章和加密（实质性要求）

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

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

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

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

2.4.10 投标文件的提交

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

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

2.4.11 投标文件的补充、修改、撤回（实质性要求）

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

供应商投标文件撤回后，视为未提交过投标文件。

2.5 开标、资格审查、评标和中标

2.5.1 开标及开标程序

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

二、开标准备工作

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

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

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化交易系统进行投标文件解密。投标人未在规定的解密时间内完成解密的，按无效投标处理。

四、开标

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

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

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

2.5.2 查询及使用信用记录

开标结束后，采购人或代理机构根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3 资格审查

详见招标文件第四章。

2.5.4 评标

详见招标文件第五章。

2.5.5 中标通知书

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

二、中标通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标供应商均具有法律效力。

2.6 签订及履行合同和验收

2.6.1 签订合同

一、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

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

2.6.2 合同分包和转包（实质性要求）

2.6.2.1合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包。

采购包2：不允许合同分包。

采购包3：不允许合同分包。

采购包4：不允许合同分包。

采购包5：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：

以招标文件和最终签订合同为准

采购包2：

以招标文件和最终签订合同为准

采购包3：

以招标文件和最终签订合同为准

采购包4：

以招标文件和最终签订合同为准

采购包5：

以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

为全面筑牢省级数字政府安全屏障，我省已构建形成“政府主导、专业协同、权责清晰、监管有效”的一体化网络安全运营体系。采购人建设的“省数字政府网络安全协调指挥及防控运营平台”已成为安全运营的核心支撑平台，实现了对政务外网（广域网、接入区、省级城域网）、各省级政务云（含政法云）和核心应用系统等的安全监测管理，并可对接各类安全监测数据集中分析与响应处置管理。为进一步提升整体安全防护能力，本项目拟通过专项采购，围绕以下四大方向推进能力升级：一是拓展监测广度，实现省级政务云机房及云上业务的全面覆盖，构建全域感知、精准溯源的风险监测体系；二是强化数据赋能，依托统一日志审计平台，集约化提供全景日志服务，增强安全数据分析与利用能力；三是聚焦新兴风险，专项开展政务大模型安全评估与监测，引入专业化安全运营服务，应对新型技术场景下的安全挑战。四是通过专业的安全运营及咨询服务，提升省级数字政府网络安全管理运营能力。通过上述举措，最终实现网络安全风险的“可监测、可预警、可处置、可追溯”，达成“可视、可管、可控”的闭环管理目标。

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）：1,188,400.00
采购包最高限价（元）：1,188,400.00
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	信息技术咨询服务（网络安全管理监督服务）	100	1,188,400.00	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）：10,215,500.00
采购包最高限价（元）：10,215,500.00
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	网络安全管理技术运营服务（工具支撑及基础运营服务）	1.00	10,215,500.00	项	软件和信息技术服务业	否	否	否	否
---	---------------------------	------	---------------	---	------------	---	---	---	---

采购包3：

采购包预算金额（元）：445,600.00

采购包最高限价（元）：445,600.00

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	终端行为分析服务	1.00	445,600.00	项	软件和信息技术服务业	否	否	否	否

采购包4：

采购包预算金额（元）：712,500.00

采购包最高限价（元）：712,500.00

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	网络和数据安全风险评估服务	1.00	712,500.00	项	软件和信息技术服务业	否	否	否	否

采购包5：

采购包预算金额（元）：1,666,600.00

采购包最高限价（元）：1,666,600.00

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	网络安全测试服务	1.00	1,666,600.00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：信息技术咨询服务（网络安全管理监督服务）

序号	参数性质	技术参数与性能指标
		一、项目概况

信息技术咨询服务（网络安全管理监督服务）等8个信息技术咨询服务

二、服务内容清单

序号	服务名称	数量	单位	服务期
1	网络安全管理监督咨询服务	1	项	8个月
2	网络安全管理评价规范服务	1	项	8个月
3	网络安全管理运营服务供应链管理服务	1	项	8个月
4	网络安全管理技术运营合规审计服务	1	项	8个月
5	地市政务云网安全摸查分析服务	1	项	8个月
6	安全管理推广服务	1	项	8个月
7	应急预案服务	1	项	8个月
8	应急演练服务	1	项	8个月

三、服务目标

1.网络安全管理监督咨询服务

构建并优化网络安全管理监督咨询体系，制定实施细则与跨部门协同机制。开展信息系统、网络平台及数据应用的全要素安全审查，识别技术漏洞、管理缺陷与合规差距。提供针对性风险管控方案，指导并督促责任单位落实整改。评估运营效能，推动社会力量参与评价，提出资源配置优化建议。归集评估数据与整改进展，形成综合报告与政策建议，支撑监管决策。

2.网络安全管理评价规范服务目标

研究制定或修订数字政府项目绩效评估模型、指标体系及管理办法。实施全过程绩效监督与关键节点评估，开展项目后评估。综合评价全省数字政府整体发展成效。组织重点领域第三方专项评估，实施监督与质量控制。分析评估结果，识别问题短板，提出改进建议。

3.网络安全管理运营服务供应链管理服务目标

开展服务方安全风险评估，覆盖资质、制度、技术等关键要素。实施运营服务全流程监管评估，量化评价服务进度与质量。整合评估数据，为服务方考核评级与合同决策提供依据。

4.网络安全管理技术运营合规审计服务目标

开展安全策略与运营总体审计，评估制度完备性与执行规范性。实施技术措施专项审计，核查配置合规性及运行有效性。

5.地市政务云网安全摸查分析服务目标

完成杨凌示范区、汉中市、渭南市、安康市、商洛市、铜川市等6个地市的政务云网安全线下摸查分析，涵盖安全架构、等级保护、密码安全、业务上云、安全运营等方面，形成总结报告并提出规划建议。

6.安全管理推广服务目标

面向全省数字政府及地市安全管理人员，开展安全意识、政策法规、风险应对等培训，服务期内组织线下集中推广不少于1次、线上视频推广不少于2次，交付培训视频、过程资料、签到记录及反馈表等材料。

7.应急预案服务目标

制定核心业务应用系统应急预案，覆盖不少于5个应急场景，明确事件级别、组织架构、责任分工与响应流程，实现在线知识库维护与流程在线流转。

8.应急演练服务目标

组织应急预案实战演练，模拟突发事件场景，检验应急机制与协调能力，每场景演练不少于1次，交付场景方案、总结报告及演练脚本等材料。

四、服务要求

包含网络安全管理监督咨询服务、网络安全管理评价规范服务、网络安全管理运营服务供应链管理服务、网络安全管理技术运营合规审计服务、地市政务云网安全摸查分析服务、安全管理推广服务、应急预案服务、应急演练服务。在服务期间采购人根据实际情况产生的相关合理需求，供应商应及时响应，不增加额外服务费用。

1、网络安全管理监督咨询服务

1.1 服务目标

构建权责清晰、监督有效、协同联动的数字政府网络安全运营管理机制。通过专业化的监督评估与风险管理服务，体系化保障省级数字政府基础设施与应用安全可靠运行，精准识别并有效管控各类安全风险与管理隐患，为省级主管部门强化监管与考核提供决策支撑，持续提升全省数字政府网络安全综合防护能力和精细化治理水平。

1.2 服务内容

监督咨询体系建设与优化：参照省级网络安全管理监督检查规范，细化制定实施细则、操作指引及跨部门协同机制。

网络安全风险评估与识别：对信息系统、网络平台、数据应用等开展全要素安全审查，精准识别技术漏洞、管理缺陷及合规差距。

风险管控方案咨询：依据风险评估结论，研提针对性管控措施与优化方案，指导并督导责任单位落实风险整改。

运营效能评估与多方协同引导：协助构建社会力量参与的评价机制，科学评估现有运营效能，包括（网络安全管理技术运营服务、终端行为分析服务、安全摸底及应急服务、网络和数据安全风险评估服务、网络安全测试服务、攻防演练服务）提出资源配置优化建议。

监管决策支撑服务：系统归集阶段性评估数据、整改进展及治理成效，形成综合报告与政策建议，支撑省级主管部门开展监管决策、绩效考核及制度修订。

1.3 服务频次

常态监督：服务期限内周期性监督检查与风险评估跟踪不少于1次。

专项深度检查：针对重点项目、高风险领域或突发事件，提供专项深度检查服务不少于1次。

报告与汇报：服务期限内提交综合评估报告1次，专项评估报告不少于1次。

实时咨询响应：对日常监管中的政策咨询、问题研判提供按需响应支持。

1.4 服务标准

合规性、专业性、客观性、精准性、时效性、保密性。

1.5 服务成果

《监督检查与风险评估综合报告》1份；

《专项网络安全风险评估报告》不少于1份；

《风险管控措施建议与整改优化方案》不少于4份；

《社会力量参与网络安全运营效能评估报告与优化建议》不少于1份；

专项咨询建议书不少于8份；

《网络安全风险识别清单与管控进展台账》不少于5份；

附加多媒体化管理数据分析展示。

2、网络安全管理评价规范服务

2.1 服务目标

构建并完善科学、全面、可操作的数字政府项目绩效评估体系。强化项目从立项到验收全过程及各关键环节的绩效管理能力，实现对省级数字政府整体发展成效的客观、精准、综合性考核评价，促进项目管理水平提升、财政资金使用效益最大化及数字政府发展目标达成。

2.2 服务内容

绩效评估体系构建与优化：研究制定/修订完善省级数字政府项目及整体发展的绩效评估模型、指标体系、操作规范和管理办法。

全过程绩效监督与评估：在项目关键里程碑节点设置绩效评估点，对项目执行过程进行动态追踪和绩效评价，项目完成后进行后评估。

数字政府整体发展成效综合考核评价：整合各项目及专项评估结果，对全省数字政府建设的整体水平、发展进程和综合效益进行周期性评价。

重点领域第三方专项评估的组织管理：协助识别需引入第三方评估的重点领域，制定评估规范，组织实施委托，并对评估过程进行监督协调和质量控制。

监督效能分析与建议：分析各项目（网络安全管理技术运营服务、终端行为分析服务、安全摸底及应急服务、网络和数据安全风险评估服务、网络安全测试服务、攻防演练服务）绩效评估结果，识别问题与短板，提出改进建议。

2.3 服务频次

绩效评估体系维护：服务期限内不少于1次；

全过程绩效监控：常态化嵌入项目管理流程，含网络安全管理技术运营服务、终端行为分析服务、网络和数据安全风险评估、网络安全测试服务；

项目后评估：项目完成后一次性进行；

整体发展成效综合考核：每年一次；

第三方专项评估：服务期限内不少于1次；

成果汇报与建议：服务期限内不少于2次。

2.4 服务标准

政策依循性、系统性完整性、科学性合理性、客观公正性、操作规范性、时效有效性、结果实用性。

2.5 服务成果

《数字政府项目绩效评估体系规范》不少于1份；

《项目关键节点绩效评估报告》不少于1份；

《项目后评估报告》1份；

《省级数字政府整体发展成效综合考核评价报告》1份；

《重点项目第三方独立评估报告》不少于2份；

《绩效监督与评估结果综合分析及改进建议报告》1份；

附加多媒体化管理数据分析展示。

3、网络安全管理运营服务供应链管理服务

3.1 服务目标

精准识别参与服务各方（网络安全管理技术运营服务、终端行为分析服务、安全摸底及应急服务、网络和数

据安全风险评估服务、网络安全测试服务、攻防演练服务）的供应链外包安全风险，为风险处置和准入管理提供依据。对运营单位服务执行情况进行全过程、多维度、客观量化的绩效评价，为省主管部门实施服务方考核与服务费用核算提供坚实的数据支撑和事实基础。

3.2 服务内容

供应链外包安全风险评估：明确纳入评估的服务方范围，对其安全资质、管理制度、技术保障等关键要素进行风险评估，识别关键风险点并评估风险等级。

运营服务全流程监管评估：基于全流程监管评估机制，持续收集、核实相关数据与证据，客观量化评价运营单位的服务完成进度、绩效达成度与质量水平。

考核支撑与计费参考：整合供应链风险评估结果与运营监管评估数据，形成综合性监管评估报告，为服务方考核评级、合同续签决策等提供客观依据。

3.3 服务频次

供应链外包安全风险评估：准入评估不少于5次，定期复评每年至少一次，动态评估不少于1次；

运营监管评估：常态化监测不少于3次，周期性评价不少于1次，年度综合考核1次；

报告与支撑：按需提交风险评估报告，按周期提交监管评估报告。

3.4 服务标准

合规性、客观公正性、专业性、全面性、精准性、时效性、保密性。

3.5 服务成果

《服务方供应链安全风险评估专项报告》不少于5份；

《运营服务季度/半年度监管评估报告》3份；

《年度监管评估与考核支撑综合报告》1份；

《服务方考核评级建议与计费依据说明》不少于5份；

运营服务绩效量化评价数据清单1份；

附加多媒体化管理数据分析展示。

4、网络安全管理技术运营合规审计服务

4.1 服务目标

保障省级数字政府相关安全技术运营工作持续满足安全风险控制要求，有效支撑数字政府业务安全稳定运行。精准识别并及时揭示技术措施、管理措施、运营过程及策略体系中的不合规行为、控制缺陷与管理缺失，驱动网络安全及云网运营技术管控体系的持续优化与完善。

4.2 服务内容

安全策略与运营总体审计：审查安全策略的制定、评审、发布、更新流程及执行一致性，安全组织架构与职责分工，安全管理制度体系的完备性与有效性，安全运营流程设计合理性与执行规范性，安全配置基线管理的合规性与有效性。

技术措施专项审计：依据国家现行网络安全管理技术规范，深入核查网络安全技术措施的配置合规性与运行有效性，系统排查技术措施中存在的问题、设计缺陷、配置错误、策略失效等隐患，综合评估网络安全防护体系及云网基础设施的保障能力效果。

4.3 服务频次

总体审计：每年至少一次全面审计，专项审计/复查不少于1次；

技术措施专项审计：核心系统/高危领域专项审计不少于12次，常规覆盖确保每12年完成一次深度技术审计，专项触发审计不少于1次；

报告提交：审计完成后20个工作日内出具正式报告。

4.4服务标准

合规权威性、独立性客观性、专业严谨性、全面系统性、风险导向性、深度穿透性、建议可行性、保密性。

4.5 服务成果

《安全策略与运营总体审计报告》1份；

《网络安全技术措施专项审计报告》不少于1份；

《重大网络安全风险隐患专项审计报告》不少于1份；

《审计发现事项及整改建议清单》不少于1份；

《审计整改情况跟踪验证报告》不少于1份；

《网络安全及云网运营保障效能评估意见》不少于1份；

附加多媒体化管理数据分析展示。

5、地市政务云网安全摸查分析服务

完成面向全省6个地市（杨凌示范区、汉中市、渭南市、安康市、商洛市、铜川市）的政务外网管理单位线下政务云网安全摸查分析工作，摸查分析各地市数字政府安全保障情况、安全现状等，并基于分析成果完成规划建设等工作。完成所有摸查分析后输出1份总结报告。

在地市开展现场摸查分析工作，摸查分析内容包括但不限于各地市政务外网网络安全架构、政务外网安全防护、等级保护建设及覆盖、密码安全建设及覆盖、业务上云、政务云安全防护、政务外网安全运营等方面。

6、安全管理推广服务

完成面向全省数字政府、地市安全管理和技术人员的集中推广工作，实现相关人员安全能力提升。

推广对象可覆盖采购人自身、采购人运维及服务单位、全省委办厅局、各地市政务外网管理单位等，视采购人实际培训需求确定培训对象，通过线下集中推广、线上视频会议等方式进行培训，服务期内线下集中推广 ≥ 1 次，线上推广 ≥ 2 次。推广内容不限于安全意识、政策及法律法规解读、国家数据局等国家层面相关政策宣贯培训、安全基础常识、安全风险应对、应急处置等方面；交付不限于视频、过程资料、活动签到表、记录表、反馈表等。

7、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，至少覆盖5个应急场景，根据采购人实际需求确定场景，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 ≥ 5 个。

8、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 ≥ 1 次。

五、设施设备配置要求

供应商应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，服务

	<p>中的各项要求为最低要求。</p> <p>供应商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所有租用服务工具数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。</p> <p>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。</p> <p>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。</p> <p>六、交付要求</p> <p>1.服务期限：自合同签订后，符合服务条件之日起8个月。</p> <p>2.付款方式：采购人采取银行转账方式按项目进度支付款项，合同签订后30日内，达到付款条件支付总金额的40%为预付款，完成交付验收后30日内，达到付款条件支付60%尾款。</p> <p>3.其他要求：</p> <p>3.1项目变更、解除和终止</p> <p>如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。</p> <p>如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。</p> <p>3.2答疑和现场考察</p> <p>本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。</p> <p>七、人员配置要求</p> <p>供应商必须针对本项目组建专项咨询服务团队人数不少于10人，其中驻场服务人员不少于4人，含驻场咨询管理人员1人、专家2人、应急服务人员1人。本项目所有人员需为供应商自有人员，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</p>
--	---

采购包2：

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。

标的名称：网络安全管理技术运营服务（工具支撑及基础运营服务）

为保障咨询工作有序开展，服务方需建立完善的咨询管理组织。应根据实际服务需求，设置相应的服务岗位，安排合适的安服务人员，每个岗位均须为服务方自有人员，以保证安全咨询服务质量。

序号	参数性质	技术参数与性能指标
		一、项目概况

二、服务内容清单

序号	服务名称	数量	单位	服务期
1	平台扩容设备租用及保障服务	1	项	3个月
2	安全监测设备租用服务	1	项	3个月
3	政务云安全监测引擎服务	1	项	3个月
4	安全监测设备租用服务（数据安全监测设备）	1	项	3个月
5	“三高一弱”重点检查服务	1	项	8个月
6	安全能力评估验证服务	1	项	8个月
7	安全资产管理服务	1	项	8个月
8	互联网安全资产测绘服务	1	项	8个月
9	安全策略运营服务	1	项	8个月
10	脆弱性采集及闭环管理服务	1	项	8个月
11	基线检查服务	1	项	8个月
12	安全编排与自动化响应服务	1	项	8个月
13	安全事件协助处置服务	1	项	8个月
14	网络安全威胁监测服务	1	项	8个月
15	安全风险资讯预警服务	1	项	8个月
16	本地情报运营服务	1	项	8个月
17	应用上线评估服务	1	项	8个月
18	应用安全监测服务	1	项	8个月
19	重大活动安全保障和值守服务	1	项	8个月
20	安全工单闭环服务	1	项	8个月
21	数据风险监测分析服务	1	项	8个月
22	接口风险监测分析服务	1	项	8个月
23	安全事件应急响应服务	1	项	8个月
24	大模型安全监测服务	1	项	8个月
25	大模型安全检测评估服务	1	项	8个月
26	公共支撑日志采集服务	1	项	3个月
27	公共支撑日志预处理服务	1	项	3个月
28	公共支撑日志审计服务	1	项	3个月
29	风险行为建模分析服务	1	项	8个月
30	攻防演练及组织服务	1	项	8个月

三、服务目标

1、平台扩容设备租用与保障目标。为构建坚实可靠的网络安全运营基础环境，确保平台服务能力与业务发展同步提升，特设定以下服务目标：

（1）完成平台资源扩容：按期完成网络安全协调指挥平台（≥12台服务器）与防控运营平台（≥2台服务器）的扩容部署。扩容后集群综合性能须满足新增数据接入要求，并预留未来一年业务拓展所需资源。

（2）保障平台持续稳定：提供涵盖证书续期、维保续期、日常巡检、组件升级及故障告警处置的全流程、一体化保障服务，确保平台年度稳定运行率不低于**99.9%**。

（3）明确交付与承诺：提交具有约束力的**平台扩容承诺函**、详尽的**扩容实施方案与系统保障方案**。按期交付**平台巡检记录、月度运行报告及运维统计表**等过程文档，确保服务过程可追溯、可考核。

2、安全监测设备租用与保障目标。为构建全方位、高性能的安全监测能力，实现对网络威胁的有效感知与响应，特设定以下服务目标：

（1）完成监测资源部署：按期部署威胁监测、漏洞扫描、全流量采集、攻击样本采集、镜像分流及非结构化数据监测等六类安全监测设备，共计**60**台，确保其覆盖范围与性能指标满足各区域的流量采集与深度分析需求。

（2）确保设备合规与互联：所有设备须为国产化硬件，性能接口符合实网部署要求，必须支持与现网协调指挥平台联动，并具备不低于**180**天的日志存储能力。

（3）落实一体化运行保障：为本项目新增及原有共计约**178**台设备，提供标准化运行保障服务，具体包括：每周远程巡检、每月现场巡检、**5×8**小时驻场运维以及**7×24**小时故障应急响应，确保监测体系持续稳定运行。

（4）明确交付与资质证明：提交各设备的详细服务方案、部署方案与专项保障方案，并同时提供所有设备的功能与技术能力证明材料，确保服务内容明确、设备资质可信。

3、政务云安全监测引擎服务目标：为构建集约化、服务化的云安全监测能力，实现对省级政务云的统一安全管控，特设定以下服务目标：

（1）建成统一监测资源池：构建覆盖多个政务云节点的云安全监测资源池，总体资源规模不低于**720**物理核、**5760GB**内存及**720TB**硬盘存储，具备不低于**150**个云内安全监测组件的接入与承载能力。

（2）实现平台核心能力：需实现统一管理门户、用户体系同步、多业务单位数据隔离与自助服务、监测组件自动化部署及应急支撑等核心功能，确保与现网协调指挥平台完成深度对接与联动。

（3）明确交付与资质验证：提交详尽的《政务云安全监测引擎服务方案》、《工具部署方案》与《系统保障方案》，并提供平台相关功能与技术能力证明材料，确保所建能力符合设计要求且可验证。

4、数据安全监测设备服务目标。为构建覆盖核心数据接口与访问行为的安全监测能力，实现对数据安全风险的精准识别与有效管控，特设定以下服务目标：

（1）完成监测能力部署：部署数据库审计工具与API接口审计工具各**10**台。其中，数据库审计工具单台性能不低于**10Gbps**，API接口审计工具单台性能不低于**8Gbps**，以满足关键业务区域的流量处理需求。

（2）确保核心分析能力：所提供的工具须具备加密流量解析、安全风险精准检测、以及细粒度的访问行为分析能力。

（3）落实标准化运行保障：对全部**20**台数据安全监测设备，提供每周远程巡检、每月现场检查、**5×8**小时驻场运维与**7×24**小时故障响应的全天候保障服务，确保监测服务连续性。

（4）明确交付与资质验证：提交完整的《数据安全监测设备服务方案》、《部署方案》与《运行保障方案》，并同时提供所有工具的官方功能与技术能力证明材料，确保设备性能与功能达标。

5、“三高一弱”重点检查与安全能力评估目标。为系统排查并化解基础性安全风险，验证关键边界防御能力有效性，特设定以下服务目标：

（1）完成全域资产风险排查：面向全省范围**24000**余个网络资产，开展“三高一弱”（高危端口、高危行为、高危漏洞、弱口令）专项检查，服务期内全面覆盖不少于**2**次，确保风险发现无遗漏。

（2）实现风险处置闭环管理：对检查发现的各类风险，通过安全平台实现从通报、整改到验证全程闭环管理，确保所有风险项整改到位并完成二次复核。

（3）开展防御能力实战验证：完成互联网及国家电子政务外网边界的防御能力评估验证，模拟覆盖不少于

12类典型攻击场景，检验并量化安全防护体系的实际有效性。

（4）明确过程与成果交付：提交详实的《专项检查实施方案》、每次检查的《专项检查报告》、服务期结束的《总结报告》，以及评估验证所用的《评估工具能力证明》，确保工作过程规范、结果可溯。

6、资产管理、策略运营与安全服务目标。为夯实安全管理基础，提升安全运营的精细化与自动化水平，特设定以下服务目标：

（1）实现资产全生命周期管理：构建覆盖全省24000余个网络资产的统一动态台账，确保资产信息实时更新、状态可知、责任可溯，实现对资产从发现、监控到退出的全生命周期管理。

（2）开展安全策略持续优化：基于威胁态势与业务需求，常态化开展安全策略运营。服务期内，策略调整与优化操作不少于11次，并同步提交《策略运营报告》，确保防御措施与时俱进。

（3）落实常态化安全运营服务：完成覆盖脆弱性采集、安全基线核查、自动化编排响应及安全事件协助处置等一系列常态化运营工作，确保对各类安全风险实现从发现、通报、处置到验证的闭环管理。

（4）确保运营过程留痕可溯：按期交付包括资产清单、风险清单、处置记录在内的各类过程文档，以及季度、年度等阶段性《安全运营总结报告》，确保所有运营活动规范透明、结果可衡量。

7、威胁监测、应急响应与专项保障目标。为构建覆盖全省关键资产的常态化监测与应急响应体系，确保网络安全风险可管、可控、可处置，特设定以下服务目标：

（1）实施全天候威胁监测：对全省关键信息资产开展7×24小时持续威胁监测，并配备5×8小时专业驻场值守，实现安全风险的实时预警、快速处置与闭环验证。

（2）提供标准化应急服务：面向各类安全事件，提供5×8小时现场协助处置服务，服务期内有效响应事件不少于120次，确保安全事件得到专业、及时的应对。

（3）落实重大活动专项保障：针对“两会”、重大节假日等关键时期，开展专项网络安全保障不少于3次，累计保障天数不低于40天，并同步提交每次保障的实施方案与总结报告。

（4）优化安全运营流程机制：完成安全工单流程的持续优化与设计，新增标准化流程不少于5个，优化现有流程不少于10个，实现安全运营工作的全流程在线化、闭环化管理。

8、大模型安全服务目标。为规范政务大模型应用，防范内容安全与数据泄露风险，确保人工智能技术在政务领域安全可靠应用，特设定以下服务目标：

（1）建立大模型安全监测体系：提供大模型安全监测服务，覆盖不超过6个政务大模型，实现对模型调用、输入输出、交互过程的全流程监测与风险识别，并确保发现的风险能够实现闭环处置。

（2）完成大模型应用安全评估：对不少于6个政务大模型应用进行上线前及运行中的安全检测评估，重点发现并评估内容安全、训练语料合规性及基础运行环境等方面的潜在风险。

（3）配备专用工具并验证能力：配套提供大模型安全监测与安全评估工具各1套。工具需支持代理接入、深度风险识别和全量行为审计，并须提交完整的官方工具能力证明材料，确保其功能与性能符合要求。

9、日志服务与行为分析目标。为构建统一、高效的日志数据治理与安全分析能力，实现对全网安全态势的深度感知与精准预警，特设定以下服务目标：

（1）建成高性能日志基础平台：完成政务外网与互联网日志服务集群的部署，形成不低于30万EPS（事件/秒）的日志采集处理能力，并覆盖不少于60个重要业务系统，确保日志数据全面汇聚。

（2）提供全流程日志数据服务：提供覆盖日志采集、标准化预处理、集中审计与综合分析的全流程服务。基于此，构建风险行为分析模型不少于10个，提升基于日志的异常行为发现与溯源能力。

（3）实现集约化服务交付：平台需支持多租户SaaS化服务模式，能够为不同业务单位提供数据隔离、权限分明的独立日志审计与分析服务。

（4）明确方案与报告交付：提交完整的《日志服务实施方案》、《日志预处理方案》、《日志审计服务方案》及《行为建模分析报告》等系列文档，确保技术路径清晰、服务过程规范、分析成果可验证。

10、攻防演练组织与服务目标。为检验并整体提升数字政府网络安全综合防御与协同应对能力，特设定以下服务目标：

（1）成功组织实战化攻防演练：策划并组织实施1次覆盖全省范围的网络安全攻防演练，确保参与攻击的队伍不少于10支，并提供演练平台、专业裁判及全过程技术保障。

（2）确保演练覆盖与成果转化：演练范围须全面覆盖省政务云业务系统及地市核心业务系统。演练中发现的所有安全风险须全部纳入协调指挥与防控运营平台，实现从通报、整改到验证的闭环管理。

（3）完成全过程资料归档与总结：提交涵盖演练方案、过程记录、问题通知单及全面总结报告在内的全套文档，确保演练过程可追溯、演练成果可衡量、后续改进有依据。

四、服务要求

开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。在服务合同履行期间，采购人因实际工作需要提出的合理需求，中标（成交）供应商予以及时响应，原则上不另行增加费用。

以下服务内容及工具要求为项目的基本质量与交付标准，供应商须对此作出实质性响应，并严格履行。供应商可在投标（响应）文件中提出有利于项目目标的优化建议，但须承诺其所提供的服务质量不低于采购文件规定的全部要求，并就此提交书面“基础要求承诺函”（格式自拟，须加盖单位公章）。

1、平台扩容设备租用及保障服务

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持续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，集群性能满足新增数据接入需求，以及未来1年新数据中心、新安全平台/工具等接入需求，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， ≥ 256 GB内存， ≥ 48 T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，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（13台服务器），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，不得影响平台的正常运行和使用。

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，包括但不限于证书续期、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：

证书续期：按要求提供服务期内有效的平台国际RSA/国密SM2证书，实现国密+国际双证书访问，保障平台的高强度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。

交付平台巡检记录、巡检报告（月报）、运维统计表等。

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。

2、安全监测设备租用服务

2.1安全监测设备服务

服务期内持续提供各类安全监测设备租用服务，服务期3个月，详见以下要求。投标需提供所有安全监测设备工具的功能证明材料（限产品截图、官网说明、第三方证明材料等）、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；提供安全场景化分析，包括对勒索病毒、弱口令、挖矿等常见安全场景的专项分析，可统计分析风险IP、风险详情。

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， $\geq 12\text{G}$ 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。

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。

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的反制溯源。

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。

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， ≥ 36 T存储空间， ≥ 128 G内存， ≥ 10 G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OCR识别，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。

2.2 安全监测设备工具保障要求

为本项目所提供的60台安全监测设备工具、原有平台相关前置系统118台，共计约178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。

为本次项目所提供的安全监测设备工具提供所必须的组网交换机，不少于4个千兆交换机，2个万兆交换机，其中千兆交换机不少于24个千兆电口，不少于4个千兆光口，万兆交换机不少于24个万兆光口，交换机性能能满足监测设备工具组网和正常运行需求。

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。

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。

3、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，服务期3个月，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政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点4（过渡）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。

须为本项目所提供的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。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：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。

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。

▲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。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。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。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。

▲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。

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。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；

▲支持实时基于业务云主机资产监控状态，展示资产健康度、资产类型分布、资产重要性分布等，并支持对云主机资产详情进行查看和配置。

▲提供安全场景化分析，包括对勒索病毒、弱口令、挖矿等常见安全场景的专项分析，可统计分析风险IP、风险详情。

4、安全监测设备租用服务（数据安全监测设备）

服务期内持续提供数据安全监测设备租用服务，服务期3个月，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）数据库审计工具服务

服务期内提供数据库审计工具服务，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。

2）API接口审计工具服务

服务期内提供API接口审计工具服务，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，支持API自动打标、支持动态API请求路径自动合并。

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。

3) 数据安全监测设备工具保障要求

为本项目所提供的20台数据安全监测设备工具，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。

升级：对相应设备进行版本升级，保证系统处于最新状态，同类设备的系统版本保持一致。

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。

5、“三高一弱”重点检查服务

完成采购人管理的省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点3（政法）、省政务云西咸节点4（过渡）、省政务云延安新区节点1（灾备）、西咸广电机房等基础设施资产、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+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、专项检查报告、服务期结束总结报告。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持续优化，按现场实际需求，持续优化漏洞批量管理、复测能力，基于检查经验和过程，对现网防控运营平台功能进行持续优化，对检查服务开展情况、进度、成果展示能清晰展示，按现场实际需求，持续实现服务进度、过程、结果的管理和呈现。

6、安全能力评估验证服务

完成采购人管理的为省数字政府的互联网边界（省政务云西咸节点4、西咸广电机房）、省政务云西咸节点1、省政务云西咸节点2与国家电子政务外网边界网络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，交付评估报告。

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；供应商自备专业评估工具，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。

7、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，含省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点3（政法）、省政务云西咸节点4（过渡）、省政务云延安新区节点1（灾备）、西咸广电机房等基础设施资产、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+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。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持续优化，包括但不限于新增展示界面、新增数据呈现等；基于服务过程中的等保密评管理需求，对现网协调指挥平台的等保密评管理功能持续进行优化，包括但不限于界面优化、新增字段、新增数据呈现等。

8、互联网安全资产测绘服务

完成采购人管理的陕西省数字政府所有政务互联网业务、对外映射资产的测绘，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；供应商需自备专用工具，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、风险提醒、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。

9、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251台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，≥11次调整，提供策略运营报告。需能根据服务成果，整合平台现有数据，对平台进行优化，与运营服务内容、成果深度融合，按现场实际需求，持续对运营可视化进行优化，包括但不限于新增展示界面、新增数据呈现等。

10、脆弱性采集及闭环管理服务

完成省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点4（过渡）等省级政务云部署的部门业务应用系统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。

11、基线检查服务

完成采购人管理的自有应用系统、上云各业务单位所有云主机的按需检查，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、服务期内总结报告。

12、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≥5个场景分析设计和≥5个脚本配置或优化，完成报告输出。

13、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≥120次；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。

14、网络安全威胁监测服务

完成采购人管理的省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点3（政法）、省政务云西咸节点4（过渡）、省政务云延安新区节点1（灾备）、西咸广电机房等基础设施资产、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+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秦政通对接、通报、预警、通知等功能进行持续优化，包括但不限于界面优化、新增展示页面、字段优化等。

15、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，可兼容新秦政通进行推送。交付不限于资讯周报、年度汇总报告，服务期内周报交付≥33份。

16、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。

17、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，手段包括但不限于漏洞扫描、渗透测试等，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；服务期内覆盖50个业务系统，上线评估报告≥50份。

18、应用安全监测服务

完成采购人管理的各数据中心的主要互联网240余个站点的安全监测服务，兼容考虑后续迁移上云站点，服务期内最大不超过300个站点，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、身份证信息等敏感内容监测；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。

19、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、护网、重要会议等）、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；服务期内重保次数≥3次，重保天数≥40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。

20.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≥5个，服务期内更新优化≥10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，对长期停滞工单节点进行催办，采用人工电话、短信、秦政通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持续优化，按现场实际需求，持续完成工单办理、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、抄送等方面。

21、数据风险监测分析服务

完成采购人管理的自有业务系统、委办局申请业务系统的7×24小时数据风险监测分析服务，对省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点3（政法）、省政务云西咸节点4（过渡）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。服务期内，完成对接现网数据安全平台，按现场实际需求，持续优化数据安全、监测分析预警等能力，包括但不限于界面优化、新增数据字段等。

22、接口风险监测分析服务

完成采购人管理的自有业务系统、委办局申请业务系统的7×24小时接口安全监测服务，对省政务云高新节点1（过渡）、省政务云西咸节点1（电信）、省政务云西咸节点2（联通）、省政务云西咸节点3（政法）、省政务云西咸节点4（过渡）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，供应商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。

23、安全事件应急响应服务

协助采购人完成自有81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≥8份，每份报告提交时间小于2天。基于应急管理需求，对现网协调指挥平台进行持续优化，实现在线应急场景化管理，可基于平台实现安全应急管理流程和联系人，衔接应急流程各个角色。

24、大模型安全监测服务

服务期内提供大模型安全监测服务，实现省级数字政府的政务相关大模型安全监测，针对人工智能大模型的调用和服务过程进行全流程监测，及时发现潜在的安全风险隐患，服务期内按要求覆盖采购人要求覆盖的大模型，不超过6个大模型，交付月度安全监测分析报告。

对政务大模型的调用进行全流程监测，符合国家网信办相关合规要求，提供配套的大模型安全监测服务工具，实现对大模型传输敏感数据内容的识别检测、针对大模型提示词的注入攻击行为检测、大模型请求调用日志的全量调用、大模型会话溯源等全过程监测，并对发现的潜在安全风险进行汇总归类，通过网络安全协调指挥平台下发至相关责任人员，并跟进风险问题至完成复测闭环。

配套提供大模型安全监测服务工具1套，工具需支持不限制类型、数量的大模型安全监测能力，覆盖政务外网和政务互联网的大模型使用环境，兼容采购人当前管理的所有政务云上运行或调用的政务大模型，能够以代理模式介入政务大模型的请求调用全过程，能够和协调指挥平台联动，兼容信创云环境部署。

工具支持能力如下：大模型全流程监测，支持对常见大模型接口的API接口代理，实现大模型调用、聊天等全流程监测；

▲大模型敏感数据监测：支持对大模型用户提问、模型推理、模型返回内容监测，对违规输入输出内容、敏感数据等识别和预警。

大模型相关攻击监测：支持对大模型提示词注入、漏洞攻击等监测，实现安全风险监测预警。

▲大模型聊天审计：支持对大模型的用户聊天内容进行全量记录，不限于时间、请求IP地址、调用模型、请求内容、返回内容、消耗Token等，并支持对单次聊天内容进行时间轴穿透关联审计。

25、大模型安全检测评估服务

服务期内提供大模型安全检测评估服务，对人工智能大模型政务应用完成进行安全风险评估，服务期内完成6个政务应用大模型评估，交付≥6份评估报告。

在政务大模型上线、政务应用上线大模型应用或功能时进行检测评估，符合国家网信办相关合规要求，提供配套的大模型安全检测评估服务工具，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大模型内容安全风险、大模型训练语料风险、大模型基础运行环境（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，通过网络安全协调指挥平台下发至相关责任人员，并跟进风险问题至完成复测闭环。

配套提供大模型安全评估服务工具1套，工具支持不限制类型、数量的大模型安全风险评估分析能力，实时进行数据采集，持续进行大模型的安全风险评估，覆盖政务外网和政务互联网的大模型使用环境，兼容采购人当前管理的所有政务云上运行或调用的政务大模型，能够和协调指挥平台联动，兼容信创云环境部署。

工具支持能力如下：▲大模型内容安全检测：支持对常见大模型的内容安全检测能力，对大模型的违规内容检测，评估大模型的稳定性、抗干扰性、抵御恶意输入能力、错误回答率等，评估大模型生成内容是否准确，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。

基础环境检测：支持大模型探测能力，可发现在运行的大模型，对大模型的基础运行环境如大模型应用、大模型服务框架等进行扫描评估，发现如Ollama漏洞等框架漏洞；语料风险检测评估：支持大模型训练语料风险的在线、离线检测能力，可检测语料中隐含的敏感内容。

26、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，覆盖至少60个待采集重要业务系统，通过日志服务平台工具覆盖省级各

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。服务期内提供1份日志采集服务汇总报告。

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、 $\geq 1280\text{GB}$ 内存， $\geq 900\text{TB}$ 存储空间， $\geq 30\text{wEPS}$ 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、 $\geq 1024\text{GB}$ 内存， $\geq 700\text{TB}$ 存储空间， $\geq 24\text{wEPS}$ 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。

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 $\geq 50000\text{EPS}$ ，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 $\geq 20\text{T}$ ，内存 $\geq 64\text{G}$ 。

日志服务工具需满足：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。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。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。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。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。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。

27、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。提交日志数据格式标准、1份日志预处理报告、季度数据预处理报告。

协助采购人持续修订统一日志数据格式标准，作为省级数字政府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。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。

需按以上要求提供服务方案。

28、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。交付1份日志模型报告、季度日志服务总结报告、年度总结报告。

面向各业务单位所提供的日志审计服务需满足：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。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。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。

▲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。

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。

面向采购人所提供的日志服务能力需额外满足：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。

▲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。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。

29、风险行为建模分析服务

服务期内基于行为分析工具，完成面向省级数字政府的日志风险行为建模分析服务，通过建立安全行为分析模型及算法，基于多源日志发现潜在的安全风险和异常行为，实现日志行为风险识别、预警，更精准的完成异常行为风险分析和定位。服务期内交付建模报告、季度风险行为分析报告。

基于行为分析工具进行日志建模分析，建立常见安全场景的日志行为风险分析模型，服务期内≥10个，并基于模型完成日志行为风险分析，提升安全内控和行为风险预警能力。工具需覆盖政务外网和政务互联网，开展试点建模分析工作，工具需具备≥4个千兆电口，≥4个万兆光口，政务外网工具硬件需满足≥96物理核、≥768GB内存，≥288TB存储空间，政务互联网工具需满足≥32物理核、≥256GB内存，≥96TB存储空间。

工具支持能力如下：通过数据关联、数据过滤等编排方式建立行为特征，对基于日志的异常行为进行关联分析，支持时间对比；可针对多个异常行为模型进行探查，查看异常时间线、列表等；

▲针对特定用户账号提供行为画像，展示包括但不限于风险评分、风险趋势图、时间轴等，提供可视化图表分析。

提供风险行为建模分析服务方案，内容需覆盖异常行为建模推荐场景（≥10种异常场景，描述场景分析思路 and 实

现效果），风险行为建模分析服务方案。

30、攻防演练及组织服务

完成省政务云所有业务系统、各地市核心业务系统（每地市至少3-5个）为范围的网络安全攻防演练活动，服务期内开展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、会议服务、文化宣传服务等；承担不限于活动相关设备租赁、场地搭建、场地安保、演练场地租赁、参会人员活动期间食宿、邀请专家、活动奖金、活动记录片等费用；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≥10支攻击队，每队≥3名攻击队员，提供场地≥150平；活动裁判≥3人、现场支撑人员≥10人，应急支撑人员≥3人；演练开始时间、周期、具体内容根据采购人需求确定。

服务方在攻防演练活动期间配套提供攻防演练平台，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）。

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；供应商需提供全过程文档样例。

五、设施设备配置要求

供应商应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，服务中的各项要求为最低要求，服务期间须根据采购人的实际网络及业务情况提供相应的服务如更换匹配的高性能工具、增加安全工具等，满足安全管理所需，不增加任何费用。

供应商所提供的所有租用设备服务工具，需从服务工具完成上架，且能正常提供服务开始计算服务期。

供应商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所有租用服务工具数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

六、交付要求

1.服务期限：第1、2、3、4、26、27、28项服务期限，自合同签订之日起3个月；其他项服务期限，自合同签

	<p>订后，符合服务条件之日起8个月。</p> <p>2.付款方式：采购人采取银行转账方式按项目进度支付款项，合同签订后30日内，达到付款条件支付总金额的40%为预付款，完成交付验收后30日内，达到付款条件支付60%尾款。</p> <p>3.其他要求：</p> <p>3.1项目变更、解除和终止</p> <p>如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。</p> <p>如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。</p> <p>3.2答疑和现场考察</p> <p>本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。</p> <p>七、人员配置要求</p> <p>供应商必须针对本项目组建专项安全技术服务团队，驻场服务人员不少于16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12人。本项目所有人员需为供应商自有人员，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。</p> <p>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。</p>
--	---

采购包3：

标的名称：终端行为分析服务

序号	参数性质	技术参数与性能指标															
		<div>一、项目概况</div> <div>终端行为分析服务等2项分析服务</div> <div>二、服务内容清单</div> <table><tr><th>序号</th><th>服务名称</th><th>数量</th><th>单位</th><th>服务期</th></tr><tr><td>1</td><td>终端行为分析服务</td><td>1</td><td>项</td><td>8个月</td></tr><tr><td>2</td><td>终端合规监控服务</td><td>1</td><td>项</td><td>8个月</td></tr></table> <div>三、服务目标</div> <div>1.终端行为分析服务目标。为构建覆盖全省政务终端的安全运营能力，实现终端行为可知、风险可控、运维可管，特设定以下服务目标：</div> <div>（1）建立终端安全监控体系：面向省数据和政务服务局、省数据和政务服务中心、政务云网及公共支撑等关键运维终端，建立终端行为安全监控与分析体系，服务期内覆盖不少于500个终端点位，并按月输出《终端行为安全分析报告》。</div> <div>（2）部署国产化分析工具：提供1套终端行为分析服务工具，须全面兼容国产化办公环境及信创云部署要求，完成与网络安全协调指挥平台实现有效对接；一次性交付终端行为分析系统工具。</div>	序号	服务名称	数量	单位	服务期	1	终端行为分析服务	1	项	8个月	2	终端合规监控服务	1	项	8个月
序号	服务名称	数量	单位	服务期													
1	终端行为分析服务	1	项	8个月													
2	终端合规监控服务	1	项	8个月													

2.终端合规监控服务目标。为强化政务终端保密管理能力，构建涉密信息防泄漏技术屏障，特设定以下服务目标：

（1）建立分级保密监控体系：分别为省数据和政务服务局（≥50个终端）及省数据和政务服务中心（≥150个终端）部署保密合规监控服务提供必要服务工具，实现对网络攻击窃密与涉密信息泄露风险的实时监测与核查，按季度输出《终端保密合规监控报告》。

（2）部署专用保密监管工具：部署1套保密安全自监管系统（含互联网自监管平台、客户端及监测引擎），支持为局、中心分别建立独立管理权限，实现终端保密自查与风险分级管理；一次性交付终端保密自监管系统工具（含工控机设备，设备含国产可控处理器，内存≥32G，硬盘≥2TB，千兆电口≥4个，千兆光口≥4个，含必要配件）。

（3）形成保密风险处置闭环：建立监测、告警、核查、处置的全流程管理机制，确保保密风险及时发现、有效处置。

四、服务要求

开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。

1、终端行为分析服务

提供终端行为分析服务，针对省数据和政务服务局、省数据和政务服务中心、政务云网、公共支撑等运维终端在日常工作中的安全行为进行监控分析，确保不发生安全行为事件。服务期内提供≥500点行为分析服务。按月交付分析报告。

提供1套终端行为分析服务工具，兼容国产化办公环境，兼容信创云部署环境，可支持与网络安全协调指挥平台对接，并提供包括终端准入管理、基线安全、威胁情报检测、黑客入侵分析等能力，对终端安全行为分析风险及时通报并处置，避免对政务云网运行造成安全风险威胁，完成风险问题的跟进闭环。

工具支持能力如下：

终端资产管理：可针对业务终端进行安全管理，包括但不限于终端资产环境信息采集、进程管理、性能监控、账号管理、应用管理等；可查看和管理所有终端的漏洞情况，并进行漏洞结果查看和导出；基线安全：提供对终端操作系统、数据库、中间件等基线安全检查，并提供安全建议；终端防病毒：支持常见类型的病毒实时防护、定时查杀。风险自评估：可评估终端安全风险，包括但不限于弱口令、高危漏洞、风险进程、高危端口、风险账户等；黑客入侵防护：可针对黑客常见的等入侵行为进行检测、告警和阻断；主机访问控制：可针对终端访问提供细粒度的访问控制，可基于黑白名单或IP地址、端口、协议、流量方向等控制因子进行访问控制；威胁情报检测：可对访问IP、域名、可疑文件等进行威胁情报匹配检测；数据防泄漏：可识别常见敏感内容，支持OCR识别，支持红头文件、印章识别，可管控即时通讯、拷贝、网盘、剪贴板、邮件、FTP等渠道，提供敏感行为阻断、审批、审计等，可备份敏感文件备查，支持对敏感数据的分级管控，可自定义终端水印，对拍照、打印等。

2、终端合规监控服务

提供终端合规监控服务，提供终端合规监控服务，针对省数据和政务服务局、省数据和政务服务中心的管理终端提供安全保密合规监控服务，进行终端涉密信息监测，接收网络攻击窃密和涉密信息检测告警事件，并上报相关监测数据，对窃密事件告警进行核实，掌握自身安全保密风险。服务期内为省数据和政务服务局提供≥50个点，为省数据和政务服务中心提供≥150个点的合规监控服务。一次性交付终端保密自监管系统工具，提供季度合规监控服务报告。

提供1套保密安全自监管服务工具，含互联网自监管平台、客户端、监测引擎等，考虑保密工作的特殊性，由于系统特殊性，需按照一次性服务工具方式交付，支持为局、中心独立划分管理组织，局、中心可分别管理各自的保密终端和掌握各自的终端保密自查情况。

工具支持能力如下：网络出口安全保密检测能力：支持在互联网出口部署互联网出口保密检测硬件工具，实现传输涉密检测、攻击涉密检测、指定对象审计、网络行为审计等；传输涉密检测：支持对网页、电子邮件、即时通讯、社交网络、HTTP、FTP、SMB协议等在线传输行为检测，检测其中涉及的敏感词，实现精准告警；攻击涉密检测：支持识别网络窃密木马、远程木马、僵尸网络、网络蠕虫、间谍程序、黑客后门、渗透行为、恶意程序/文档攻击等基于网络的攻击窃密行为，并进行告警；指定对象审计：支持对IP、域名、URL、用户邮件账号等指定对象的审计，可针对性审计对应对象会话；网络行为审计：支持对会话访问情况、网络Web访问、邮件传输、DNS域名请求、及时消息、文件传输等网络行为的全量审计；终端保密检测能力：支持终端保密检测组件，兼容国产化终端环境部署，支持托盘图标展示，可支持一键自查、敏感文件告警、终端异常行为告警等能力；一键自查：支持对涉密敏感信息的一键自查能力，可基于文件、文件操作记录、上网记录、移动介质、终端详情等维度进行自查，并输出详细的自查结果报告；敏感文件告警：支持对敏感涉密文件、疑似文件、非密文件的列表管理，可监控疑似、涉密文件的重命名、删除、复制、剪切等操作，并进行告警，支持对文本、图片、网页、音视频、压缩包等常见格式文件进行抓取，支持图片OCR识别、支持音视频内容检测；终端异常行为告警：支持对终端的出网流量进行审计，对涉及涉密文件、疑似文件外流的进行告警，支持基于预设行为策略对终端、人员、应用、数据、账号等维度进行数据统计和数据挖掘，基于预设行为基线实现用户异常行为研判告警。

五、设施设备配置要求

供应商应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，服务中的各项要求为最低要求，服务期间须根据采购人的实际网络及业务情况提供相应的服务如更换匹配的高性能工具、增加安全工具等，满足安全管理所需，不增加任何费用。

供应商所提供的所有租用设备服务工具，需从服务工具完成上架，且能正常提供服务开始计算服务期，根据实际情况提供配套设备，满足使用要求。

供应商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所有租用服务工具数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

六、交付要求

	<p>1.服务期限：自合同签订后，符合服务条件之日起8个月。</p> <p>2.付款方式：采购人采取银行转账方式按项目进度支付款项，合同签订后30日内，达到付款条件支付总金额的40%为预付款，完成交付验收后30日内，达到付款条件支付60%尾款。</p> <p>3.其他要求：</p> <p>3.1项目变更、解除和终止</p> <p>如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。</p> <p>如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。</p> <p>3.2答疑和现场考察</p> <p>本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。</p> <p>七、人员配置要求</p> <p>供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于5人，并提供每周1人/天驻场服务提供终端安全风险处置服务。本项目所有服务人员需为供应商自有人员，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。</p> <p>为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。</p>
--	---

采购包4：

标的名称：网络和数据安全风险评估服务

序号	参数性质	技术参数与性能指标															
		<div>一、项目概况</div> <div>网络和数据安全风险评估服务等2项风险评估服务</div> <div>二、服务内容清单</div> <table><tr><th>序号</th><th>服务名称</th><th>数量</th><th>单位</th><th>服务期</th></tr><tr><td>1</td><td>网络安全风险评估服务</td><td>1</td><td>项</td><td>8个月</td></tr><tr><td>2</td><td>数据安全管理服务（数据安全风险评估）</td><td>1</td><td>项</td><td>8个月</td></tr></table> <div>三、服务目标</div> <div>1.网络安全风险评估服务目标</div> <div>围绕提升核心系统及上云重要应用的安全防护能力，开展全面风险评估工作，达成对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、影响及衍生风险等多个维度，依据国家标准开展安全技术与管理方面的综合风险评估。服务期内完成20个系统的风险评估工作。产出内容包括风险评估方案、评估报告及过程资料，并通过协调指挥与防控运营平台实现在线流转与过程管理。对评估发现的安全风险，推动整改并完成修复结果的二次验证，形成风险管理闭环。服务期内交付符合要求的风险评估报告不少于20份。</div>	序号	服务名称	数量	单位	服务期	1	网络安全风险评估服务	1	项	8个月	2	数据安全管理服务（数据安全风险评估）	1	项	8个月
序号	服务名称	数量	单位	服务期													
1	网络安全风险评估服务	1	项	8个月													
2	数据安全管理服务（数据安全风险评估）	1	项	8个月													

2.数据安全管理服务（数据安全风险评估）目标

围绕局和中心核心系统及上云重要应用的安全，系统识别并有效管控核心业务系统数据安全风险，提升整体数据安全防护水平，特设定以下服务目标：

（1）完成数据风险评估：依据国家标准，对采购人管理的核心系统及上云重要应用系统，从资产、威胁、脆弱性、影响及衍生风险等多个维度，开展安全技术与管理方面的综合风险评估，服务期内完成评估的系统数量为8个。

（2）实现评估过程闭环管理：通过协调指挥与防控运营平台，实现从评估方案审核、任务下发、过程管控到报告归档的全流程在线流转与管理。

（3）落实风险整改与验证：对评估发现的安全风险，推动相关责任单位完成整改，并对修复结果进行100%二次验证，确保形成完整的管理闭环。

（4）成果交付：服务期内交付内容包括《数据安全风险评估总体方案》、8份符合要求的单系统《风险评估报告》及相关过程资料，确保评估工作过程规范、结果可溯。

四、服务要求

开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。在服务期间采购人根据实际情况产生的相关合理需求，供应商应及时响应，不增加额外服务费用。

1、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20个，经审批后开展服务，服务期内每系统评估≥1次，交付评估报告≥20份。

2、数据安全管理服务（数据安全风险评估）

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≥8个，经审批后开展服务。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。服务期内评估系统8个，经审批后开展服务，服务期内每系统评估≥1次，交付评估报告≥8份。

五、设施设备配置要求

供应商应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，服务中的各项要求为最低要求。

供应商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所有数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

	<p>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。</p> <p>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。</p> <p>六、交付要求</p> <p>1.服务期限：自合同签订后，符合服务条件之日起8个月。</p> <p>2.付款方式：采购人采取银行转账方式按项目进度支付款项，合同签订后30日内，达到付款条件支付总金额的40%为预付款，完成交付验收后30日内，达到付款条件支付60%尾款。</p> <p>3.其他要求：</p> <p>3.1项目变更、解除和终止</p> <p>如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。</p> <p>如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。</p> <p>3.2答疑和现场考察</p> <p>本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。</p> <p>七、人员配置要求</p> <p>供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于7人，现场驻场服务人员不少于1人。本项目所有服务人员需为供应商自有人员，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。</p> <p>为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。</p>
--	--

采购包5：

标的名称：网络安全测试服务

序号	参数性质	技术参数与性能指标									
		<div>一、项目概况</div> <div>网络安全测试服务等2项测试服务</div> <div>二、服务内容清单</div> <table><tr><th>序号</th><th>服务名称</th><th>数量</th><th>单位</th><th>服务期</th></tr></table>					序号	服务名称	数量	单位	服务期
序号	服务名称	数量	单位	服务期							

1	渗透测试服务	1	项	8个月
2	源代码安全审计服务	1	项	8个月

三、服务目标

1.渗透测试服务目标。为通过实战化攻防验证业务系统安全防护能力，精准发现并推动化解深层安全风险，特设定以下服务目标：

（1）完成深度渗透测试：对采购人管理的自有系统及各上云业务单位系统开展深度人工渗透测试，服务期内累计完成有效测试不少于100次，全面覆盖移动APP、Web站点、小程序、CS客户端等各类业务前端。

（2）实施全面漏洞探测：测试范围须涵盖信息收集、配置管理、身份认证与会话管理、访问授权、数据验证及系统应用漏洞等关键环节，深度评估安全隐患的实际危害与漏洞可利用性。

（3）建立闭环处置机制：对发现的每个漏洞输出单系统《渗透测试报告》，提出针对性处置建议，并于测试完成后一周内提交。所有漏洞通过协调指挥与防控运营平台实现线上流转、督办与状态跟踪，并提供修复后的二次验证，确保闭环管理。

（4）提供持续风险管控：对已验证无法彻底修复的漏洞，提供明确的风险控制措施与持续监控方案。服务期内交付《渗透测试总体实施方案》及全部单系统测试报告，确保所有测试活动规范、可溯。

（5）确保服务过程规范可溯：服务期内交付《渗透测试实施方案》、100份《系统渗透测试报告》，并提供所使用工具的正规采购或租用证明材料，确保服务全程合规、结果可信。

2.源代码安全审计服务目标。为从源头上有效管控软件安全质量，系统性降低代码层与组件层安全风险，特设定以下服务目标：

（1）完成全面源代码审计：对采购人指定或按需申请的系统开展源代码安全审计，服务期内覆盖系统数量不少于20个，确保审计范围全面、无遗漏。

（2）采用专业工具与人工分析：使用专业的非开源商用源代码安全审计工具与软件成分分析工具，通过工具自动化扫描与专家人工分析相结合的方式，深度检测代码漏洞、逻辑缺陷、开源组件风险及许可协议合规性问题。

（3）实现全流程风险管控：审计内容全面覆盖输入验证、身份鉴别、授权管理、安全加密、错误处理、日志记录及逻辑结构等关键环节；成分分析涵盖组件名称、版本、已知漏洞、许可协议及依赖关系。关联利用CNVD、CNNVD、Github等主流漏洞库情报信息，协助开发人员完成问题修复并实施修复后复测验证，确保安全风险实现闭环管理。

（4）提供持续风险处置建议：对因客观条件限制无法彻底修复的安全问题，提供切实可行的风险规避与风险降低建议，并完整记录在案。

（5）确保服务过程规范可溯：服务期内交付《源代码审计总体实施方案》、20份《源代码安全审计报告》及《软件成分分析评估报告》，并提供所使用工具的正规采购或租用证明材料，确保服务全程合规、结果可信。

四、服务要求

开展以下服务项前必须提交详细的各项服务的实施方案，经采购人审核批准后方可开展服务，且服务全程须接受采购人与信息技术咨询服务（网络安全管理监督服务）方的监管，遵从各项技术规范要求；服务产生的各项交付物须经信息技术咨询服务（网络安全管理监督服务）方审核后方可提交采购人进行审核。在服务期间采购人根据实际情况产生的相关合理需求，供应商应及时响应，不增加额外服务费用。

1、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≥100次系统的人工渗透测试（每系统做一次记数量一次），经采购人审批后开展服务。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。供应商对渗透测试的结果承担责任，渗透测试过的系统在随后的攻防演练中被攻破（“0day”漏洞除外），或被安全主（监）管部门通报，且漏洞发布时间早于测试完成时间的，按照违约条款处置。

2、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。所采用的源代码安全审计和软件组件成分评估工具需为非开源的商用工具，在服务前需提供服务方采购或租用相关工具的证明材料。

五、设施设备配置要求

供应商应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，服务中的各项要求为最低要求。

供应商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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

六、交付要求

1.服务期限：自合同签订后，符合服务条件之日起8个月。

2.付款方式：采购人采取银行转账方式按项目进度支付款项，合同签订后30日内，达到付款条件支付总金额的40

	<p>%为预付款，完成交付验收后30日内，达到付款条件支付60%尾款。</p> <p>3.其他要求：</p> <p>3.1项目变更、解除和终止</p> <p>如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。</p> <p>如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。</p> <p>3.2答疑和现场考察</p> <p>本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。</p> <p>七、人员配置要求</p> <p>供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于13人，提供驻场测试服务人员不少于2人。本项目所有服务人员需为供应商自有人员，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。</p> <p>为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。</p>
--	--

3.2.3人员配置要求

采购包1：

供应商必须针对本项目组建专项咨询服务团队人数不少于**10**人，其中驻场服务人员不少于**4**人，含驻场咨询管理人员**1**人、专家**2**人、应急服务人员**1**人。本项目所有人员需为供应商自有人员，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。 为保障咨询工作有序开展，服务方需建立完善的咨询管理组织。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，每个岗位均须为服务方自有人员，以保证安全咨询服务质量。

采购包2：

供应商必须针对本项目组建专项安全技术服务团队，驻场服务人员不少于**16**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**12**人。本项目所有人员需为供应商自有人员，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。

采购包3：

供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于**5**人，并提供每周**1**人/天驻场服务提供终端安全风险处置服务。本项目所有服务人员需为供应商自有人员，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。为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。

采购包4:

供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于**7**人，现场驻场服务人员不少于**1**人。本项目所有服务人员需为供应商自有人员，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。为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。

采购包5:

供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于**13**人，提供驻场测试服务人员不少于**2**人。本项目所有服务人员需为供应商自有人员，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。为保障服务工作有序开展，服务方需建立完善的项目团队组织。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，每个岗位均须为服务方自有人员，以保证安全服务质量。

3.2.4 设施设备配置要求

采购包1:

供应商应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，服务中的各项要求为最低要求。供应商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所有租用服务工具数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

采购包2:

供应商应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，服务中的各项要求为最低要求。供应商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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

采购包3：

供应商应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，服务中的各项要求为最低要求，服务期间须根据采购人的实际网络及业务情况提供相应的服务如更换匹配的高性能工具、增加安全工具等，满足安全管理所需，不增加任何费用。供应商所提供的所有租用设备服务工具，需从服务工具完成上架，且能正常提供服务开始计算服务期，根据实际情况提供配套设备，满足使用要求。供应商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所有租用服务工具数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

采购包4：

供应商应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，服务中的各项要求为最低要求。供应商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所有数据（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，供应商无权使用、转让或处理服务过程、成果数据。供应商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。

采购包5：

供应商应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，服务中的各项要求为最低要求。供应商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，供应商无权使用、转让或处理服务

过程、成果数据。供应商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：
以招标文件和最终签订合同为准
- 采购包2：
以招标文件和最终签订合同为准
- 采购包3：
以招标文件和最终签订合同为准
- 采购包4：
以招标文件和最终签订合同为准
- 采购包5：
以招标文件和最终签订合同为准

3.3商务要求

3.3.1服务期限

- 采购包1：
自合同签订后，符合服务条件之日起8个月
- 采购包2：
自合同签订后，符合服务条件之日起8个月（第1、2、3、4、26、27、28项服务自符合服务条件之日起3个月）
- 采购包3：
自合同签订后，符合服务条件之日起8个月
- 采购包4：
自合同签订后，符合服务条件之日起8个月
- 采购包5：
自合同签订后，符合服务条件之日起8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
- 采购包3：
采购人指定地点
- 采购包4：
采购人指定地点

采购包5:

采购人指定地点

3.3.3考核（验收）标准和方法

采购包1:

以招标文件和最终签订合同为准。

采购包2:

以招标文件和最终签订合同为准

采购包3:

以招标文件和最终签订合同为准

采购包4:

以招标文件和最终签订合同为准

采购包5:

以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

采购包3:

分期付款

采购包4:

分期付款

采购包5:

分期付款

3.3.5.支付约定

采购包1: 付款条件说明: 采购人采取银行转账方式按项目进度支付款项, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包1: 付款条件说明: 完成交付验收后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

采购包2: 付款条件说明: 采购人采取银行转账方式按项目进度支付款项, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包2: 付款条件说明: 完成交付验收后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

采购包3: 付款条件说明: 采购人采取银行转账方式按项目进度支付款项, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包3: 付款条件说明: 完成交付验收后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

采购包4: 付款条件说明: 采购人采取银行转账方式按项目进度支付款项, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包4: 付款条件说明: 完成交付验收后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

采购包5: 付款条件说明: 采购人采取银行转账方式按项目进度支付款项, 达到付款条件起 30 日内, 支付合同总金额的 40.00%。

采购包5: 付款条件说明: 完成交付验收后, 达到付款条件起 30 日内, 支付合同总金额的 60.00%。

3.3.6违约责任与解决争议的方法

采购包1:

以招标文件和最终签订合同为准

采购包2:

以招标文件和最终签订合同为准

采购包3:

以招标文件和最终签订合同为准

采购包4:

以招标文件和最终签订合同为准

采购包5:

以招标文件和最终签订合同为准

3.5其他要求

1、项目变更、解除和终止 如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予供应商补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照合同约定公平、合理的原则共同协商修改本项目对应的合同的相关条款。2、答疑和现场考察 本项目不组织答疑会和现场考察，供应商可根据实际情况自行开展现场考察，供应商考察现场所发生的一切费用由供应商自行承担。

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 中小企业声明函 残疾人福利性单位声明函 投标文件封面 投标人应提交的相关资格证明材料 监狱企业的证明文件
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。	投标函 投标文件封面 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 投标文件封面

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 中小企业声明函 残疾人福利性单位声明函 投标文件封面 投标人应提交的相关资格证明材料 监狱企业的证明文件
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。	投标函 投标文件封面 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 投标文件封面
---	---	---------------------------------------	------------

采购包3:

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 中小企业声明函 残疾人福利性单位声明函 投标文件封面 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	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。	投标函 投标文件封面 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 投标文件封面

采购包4:

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 中小企业声明函 残疾人福利性单位声明函 投标文件封面 投标人应提交的相关资格证明材料 监狱企业的证明文件
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。	投标函 投标文件封面 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 投标文件封面
---	---	---------------------------------------	------------

采购包5:

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 中小企业声明函 残疾人福利性单位声明函 投标文件封面 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	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。	投标函 投标文件封面 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 投标文件封面

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、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》	

1	本项目的特定资格要求	<p>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2024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2025年01月01日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2025年01月01日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（提供非联合体承诺）</p>	<p>非联合体承诺书（包一）.docx 资格证明文件（包一）.docx 供应商关联承诺书（包一）.docx 投标函 中小企业声明函 残疾人福利性单位声明函 拒绝政府采购领域商业贿赂承诺书（包一）.docx 投标文件封面 监狱企业的证明文件 投标人应提交的相关资格证明材料</p>
---	------------	--	---

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
		<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</p>	

1	本项目的特定资格要求	<p>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2024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2025年01月01日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2025年01月01日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、无严重违法记录声明：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严重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（提供非联合体承诺）。</p>	<p>拒绝政府采购领域商业贿赂承诺书（包二）.docx 投标函 中小企业声明函 残疾人福利性单位声明函 供应商关联承诺书（包二）.docx 投标文件封面 非联合体承诺书（包二）.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 资格证明文件（包二）.docx</p>
---	------------	--	---

采购包3:

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2024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2025年01月01日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2025年01月01日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</p>	<p>拒绝政府采购领域商业贿赂承诺书（包三）.docx 非联合体承诺书（包三）.docx 资格证明文件（包三）.docx 供应商关联承诺书（包三）.docx 投标函 中小企业声明函 残疾人福利性单位声明函 投标文件封面 监狱企业的证明文件 投标人应提交的相关资格证明材料</p>

		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（提供非联合体承诺）	
--	--	--	--

采购包4:

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2024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2025年01月01日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2025年01月01日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	供应商关联承诺书（包四）.docx 非联合体承诺书（包四）.docx 投标函 中小企业声明函 残疾人福利性单位声明函 投标文件封面 资格证明文件（包四）.docx 拒绝政府采购领域商业贿赂承诺书（包四）.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

		业信用公示系统（ 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（提供非联合体承诺）。	
--	--	---	--

采购包5:

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 2024 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 2025年01月01日 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 2025年01月01日 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	投标函 中小企业声明函 残疾人福利性单位声明函 资格证明文件（包五）.docx 拒绝政府采购领域商业贿赂承诺书（包五）.docx 投标文件封面 非联合体承诺书（包五）.docx 供应商关联承诺

		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（提供非联合体承诺）。	书（包五）.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
--	--	--	--------------------------------------

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
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	投标函 中小企业声明函 残疾人福利性单位声明函 投标文件封面 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	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	投标函 中小企业声明函 残疾人福利性单位声明函 投标文件封面 监狱企业的证明文件

采购包3:

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	投标函 中小企业声明 函 残疾人福利性单位 声明函 投标文件封面 监狱企业的证明文件
---	----------------	----------------	---

采购包4:

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	投标函 中小企业声明 函 残疾人福利性单位 声明函 投标文件封面 监狱企业的证明文件

采购包5:

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	投标函 中小企业声明 函 残疾人福利性单位 声明函 投标文件封面 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

采购包3：综合评分法

采购包4：综合评分法

采购包5：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	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 投标函 标的清单 投标文件封面
2	投标文件签字盖章	符合招标文件签字盖章的要求	投标函 投标文件封面
3	投标响应文件有效期	投标响应文件的有效期限达到招标文件要求	投标函 投标文件封面

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 投标函 标的清单 投标文件封面
2	投标文件签字盖章	符合招标文件签字盖章的要求	投标函 投标文件封面
3	投标响应文件有效期	投标响应文件的有效期限达到招标文件要求	投标函 投标文件封面

采购包3:

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 投标函 标的清单 投标文件封面
2	投标文件签字盖章	符合招标文件签字盖章的要求	投标函 投标文件封面
3	投标响应文件有效期	投标响应文件的有效期限达到招标文件要求	投标函 投标文件封面

采购包4:

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 投标函 标的清单 投标文件封面

2	投标文件签字盖章	符合招标文件签字盖章的要求	投标函 投标文件封面
3	投标响应文件有效期	投标响应文件的有效期限达到招标文件要求	投标函 投标文件封面

采购包5:

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 投标函 标的清单 投标文件封面
2	投标文件签字盖章	符合招标文件签字盖章的要求	投标函 投标文件封面
3	投标响应文件有效期	投标响应文件的有效期限达到招标文件要求	投标函 投标文件封面

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

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

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

- （一）投标人投标文件中不应响应招标文件规定的技术参数指标和商务应答；
- （二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。
- （三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

- （一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （二）大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；

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

（四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

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

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

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

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

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

5.4.5复核

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

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

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

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

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

5.4.6确定中标候选人名单

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

采购包2：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包3：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4：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5：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 and 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
	现状及需求分析	供应商提供针对本项目现状及需求分析，内容包含：①对陕西省数字政府信息技术咨询服务需求及现状的理解；②对本项目的业务现状分析；③对本项目业务需求分析。一、评审标准：（1）针对性：方案能够紧扣项目情况得 2 分，有缺陷得 1 分，未提供得 0 分。（2）合理性：方案内容符合项目实际情况，内容合理完整得 2 分，有缺陷得 1 分，未提供得 0 分。此项最高得分 4 分。二、赋分标准（满分 12 分）共 3 项内容，每项满分 4 分。按照“评审标准”，每个每满足一个评审标准得 2 分，有缺陷得 1 分，未提供得 0 分。	12.0000	主观	服务内容及服务邀请 应答表 现状及需求分析（包一）.docx 商务应答表 服务方案

服务要求响应方案	<p>供应商依据招标人所提供对本项目的①网络安全管理监督咨询服务；②网络安全管理评价规范服务；③网络安全管理运营服务供应链管理服务；④网络安全管理技术运营合规审计服务；⑤地市政务云网安全摸查分析服务；⑥安全管理推广服务；⑦应急预案服务；⑧应急演练服务，等8项服务要求进行实质性响应并进行优化提升的。一、评审标准（1）专业性：切合本项目实际情况，提出专业性强、科学合理的方案，得1分，有缺陷得0.5分，未提供得0分。（2）可实施性：切合本项目实际情况，提出步骤清晰、专业性强、合理的方案，得1分，有缺陷得0.5分，未提供得0分。（3）针对性：方案能够紧扣项目实际需求，内容科学，保障项目顺利实施，得1分，有缺陷得0.5分，未提供得0分。此项最高得分3分。二、赋分标准（满分24分）共8项，每项满分3分。按照“评审标准”，每个方案每满足一项评审标准得1分，有缺陷得0.5分，未提供得0分。</p>	24.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 服务要求响应方案（包一）.docx
服务方案	<p>供应商提供针对本项目的服务方案，方案包含：①服务目标；②服务内容；③服务频次；④服务标准；⑤服务成果。一、评审标准：（1）针对性：方案能够紧扣项目情况得1分，有缺陷得0.5分，未提供得0分。（2）合理性：内容符合项目实际，未出现与项目执行无关的内容得1分，有缺陷得0.5分，未提供得0分。此项最高得分2分。二、赋分标准（满分10分）共5项内容，每项满分2分。按照“评审标准”，每个每满足一个评审标准得1分，有缺陷得0.5分，未提供得0分。</p>	10.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表

详细评审	服务保证措施	<p>供应商提供针对本项目的服务保证措施，内容包括：①质量保证措施；②进度保证措施；③组织保障措施；④项目管理措施。一、评审标准（1）针对性：方案能够紧扣项目实际情况得2分，有缺陷得1分，未提供得0分。（2）合理性：内容符合项目实际且未出现与项目执行无关内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。</p> <p>二、赋分标准（满分16分）共4项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	16.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 服务保证措施（包一）.docx
	保密方案	<p>供应商提供针对本项目的保密方案，内容包括：①保密管理制度；②针对本项目的保密措施。一、评审标准（1）针对性：方案能够紧扣项目实际情况，得1分，有缺陷得0.5分，未提供得0分。（2）合理性：内容符合项目实际，未出现与项目执行无关的内容，得1分，有缺陷得0.5分，未提供得0分。此项最高得分2分。二、赋分标准(满分4分)共2项内容，每项满分2分。按照“评审标准”，每个每满足一个评审标准得1分，有缺陷得0.5分，未提供得0分。</p>	4.0000	主观	服务内容及服务邀请 应答表 保密方案（包一）.docx 商务应答表 服务方案

培训方案	<p>供应商提供针对本项目安全管理推广服务的培训方案，内容包括:①培训方案；②实施安排。一、评审标准（1）针对性:方案能够紧扣项目实际情况，得1分，有缺陷得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得1分，有缺陷得0.5分，未提供得0分。此项最高得分2分。二、赋分标准(满分4分)共2项内容，每项满分2分。按照“评审标准”，每个每满足一个评审标准得1分，有缺陷得0.5分，未提供得0分。</p>	4.0000	主观	<p>服务内容及服务邀请应答表</p> <p>培训方案（包一）.docx</p> <p>商务应答表</p> <p>服务方案</p>
企业实力	<p>供应商应具备与本项要求相符的服务能力，①具备工程咨询单位（电子、信息工程）备案证明；②具备信息安全服务资质认证证书。一、评审标准：提供相关证明材料，如国家权威机构体系认证证书复印件及信息查询截图证明并盖章，得2分，未提供得0分。此项最高得分2分。二、赋分标准（满分4分）共2项内容，每项满分2分。按照“评审标准”，每满足1个评审标准得2分，未提供得0分。</p>	4.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包一）.docx</p> <p>商务应答表</p> <p>服务方案</p>
团队组织架构	<p>供应商提供针对本项目拟投入的工作组成员的情况说明。内容至少包含：①工作组成员管理组织架构、人员分工;②工作职责划分、业务管理流程等内容。一、评审标准（1）针对性:内容能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。二、赋分标准(满分2分)共2项内容，每项满分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包一）.docx</p> <p>商务应答表</p> <p>服务方案</p>

	<p>供应商必须针对本项目组建专项咨询服务团队人数不少于10人；其中驻场服务人员不少于4人，含驻场管理咨询人员2人、安全专业咨询人员1人、安全应急服务人员1人，并提供投标文件驻场人员与实际驻场人员一致性承诺。在满足人员要求基础上进行以下赋分： 一、评审标准（1）项目经理：具有信息系统项目管理师证书得3分，具系统集成项目管理工程师得1分，未提供得0分。此项最高得分3分。（2）驻场人员（不含项目经理）：提供资质不得同一人员重复使用，①管理咨询人员不少于2人，具备信息化类高级工程师证明得2分；具备信息化类中级工程师证明得1分；未提供得0分。②安全专业咨询人员不少于1人，具备注册信息安全工程师（CISP）得1分，未提供得0分。③安全应急服务人员1人，具备注册应急响应工程师CISP-IRE或注册应急响应专家CISP-IRS或注册威胁响应工程师CISP-TRE或注册威胁响应专家CISP-TRS或网络安全应急响应工程师CSERE或网络安全能力认证（CCSC）等任意一项证书，得1分，未提供得0分。此项最高得分6分。（3）团队人员（除项目经理和驻场人员外）：服务人员不少于5人，提供资质不得同一人员重复使用，具有信息化类中级工程师或注册信息安全工程师（CISP、CISSP）认证，每提供1个计1分，未提供得0分；此项最高计2分。 二、赋分标准（满分11分）共3项，项目经理满分3分，驻场人员满分6分，团队人员满分2分。按照“评审标准”，项目经理提供信息系统项目管理师证书得3分，提供系统集成项目管理工程师得1分</p>				
团队力量		11.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包一）.docx</p> <p>商务应答表</p> <p>服务方案</p>	

		，未提供得0分。驻场人员提供高级工程师证明每个得2分，提供中级工程师证明每个得1分，其余资质每项提供得1分，未提供得0分。团队人员每提供一项证明材料得1分，未提供得0分。备注：需提供有效的证书复印件。			
	业绩	供应商需提供2022年01月01日（日期以签订合同实际为准）至今，承接的同类（信息化服务类）项目的业绩经验。提供采购合同复印件并加盖供应商公章。不满足要求不得分。一、评审标准：每提供一份证明材料得1分，未提供得0分，此项最高3分。二、赋分标准（满分3分）共1项内容，满分3分。按照“评审标准”每满足一个评审标准得1分，未提供得0分。	3.0000	客观	业绩（包一）.docx 商务应答表 服务方案
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.符合招标文件规定的小微企业、监狱企业、残疾人福利性单位优惠条件的供应商，价格给予10%的扣除，用扣除后的价格参与评审。5.明显低于成本价进行报价的投标视为无效投标。	10.0000	客观	分项报价表（包一）.docx 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
----	----------	------	--------------	---------	----------------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件
---	-----------------------	--------------------	--------	--	--

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

	现状及需求分析	<p>供应商提供针对本项目现状及需求分析，内容包含：①对陕西省数字政府网络安全管理技术运营服务的需求及现状的理解；②服务目标分析；③对本项目服务需求分析。一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，方案基本符合项目情况得1分，有缺陷得0.5分，未提供得0分。（2）合理性：内容符合项目实际、未出现与项目执行无关内容得2分，内容基本符合项目实际或存在部分与项目执行无关内容得1分，有缺陷得0.5分，未提供得0分。此项最高得分4分。二、赋分标准（满分12分）共3项内容，每项最高得4分。按照“评审标准”，每满足一个评审标准得2分，部分满足评审标准得1分，有缺陷得0.5分，未提供得0分。</p>	12.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 现状及需求分析（包二）.docx
	服务要求响应	<p>供应商针对招标人服务要求进行实质性响应，未提供基础要求承诺函不得分。本项目带“▲”条款内容（19项）需提交证明材料，不限产品截图、官网说明、第三方证明材料等；交付内容不限于实施方案、汇总清单、季度、年度报告等；证明材料需关联章节号及页码。一、评审标准：每项关键技术项服务“▲”内容如实响应且响应材料满足内容要求得1分，存在缺陷得0.5分，未提供得0分。此项最高得分19分。二、赋分标准（满分19分）共19项内容，满分19分。按照“评审标准”，每满足一个评审标准得1分，存在缺陷得0.5分，未提供得0分。</p>	19.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 服务要求响应方案（包二）.docx

服务方案	供应商针对本项目的服务方案，内容包含①平台扩容设备租用及保障服务；②安全监测设备租用服务；③政务云安全监测引擎服务；④安全监测设备租用服务（数据安全监测设备）；⑤公共支撑日志采集服务；⑥公共支撑日志预处理服务；⑦公共支撑日志审计服务；⑧风险行为建模分析服务等8项服务的实质性响应。一、评审标准：（1）每项服务方案内容可实施性，切合本项目实际情况，提出步骤清晰、专业性强、合理的方案，得0.5分，未提供得0分。（2）每项服务方案针对性，方案能够紧扣项目实际需求，内容科学，保障项目顺利实施，得0.5分，未提供得0分。此项最高得分1分。二、赋分标准（满分8分），共8项，每项最高得1分。按照“评审标准”，每个每满足一项评审标准得0.5分，未提供得0分。	8.0000	主观	服务内容及服务邀请 应答表 商务应答表 服务方案
------	--	--------	----	-----------------------------------

服务方案	供应商提供针对本项目的服务方案，内容包含 (1)“三高一弱”重点检查服务；(2)安全能力评估验证服务；(3)安全资产管理服务；(4)互联网安全资产测绘服务；(5)安全策略运营服务；(6)脆弱性采集及闭环管理服务；(7)基线检查服务；(8)安全编排与自动化响应服务；(9)安全事件协助处置服务；(10)网络安全威胁监测服务；(11).安全风险资讯预警服务；(12)本地情报运营服务；(13)应用上线评估服务；(14)应用安全监测服务；(15)重大活动安全保障和值守服务；(16)安全工单闭环服务；(17)数据风险监测分析服务；(18)接口风险监测分析服务；(19)安全事件应急响应服务；(20)大模型安全监测服务；(21)大模型安全检测评估服务；(22)攻防演练及组织服务的方案。一、评审标准：（1）针对性：每项方案能够紧扣项目情况得0.5分，未提供得0分。（2）完整性：每项方案能够包含服务目标、服务内容、服务交付清单及成果内容、服务频次、服务交付流程等内容，整体内容完整、符合项目实际，未出现与项目执行无关的内容得0.5分，未提供得0分。此项最高得分1分。二、赋分标准（满分22分），共22个项内容，每项满1分。按照“评审标准”，每个方案每满足一个评审标准得0.5分，未提供得0分。	22.0000	主观	服务内容及服务邀请 应答表 商务应答表 服务方案
------	--	---------	----	-----------------------------------

详细评审	服务保证措施	<p>供应商提供针对本项目的服务保证措施，内容包括：①质量保证措施；②进度保证措施；③组织保障措施；④项目管理措施；⑤风险控制措施。一、评审标准：（1）针对性：每项方案能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性：每项方案内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。二、赋分标准（满分5分）共5项内容，每项最高得分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	5.0000	主观	<p>服务保证措施（包二）.docx</p> <p>商务应答表</p> <p>服务方案</p> <p>服务内容及服务邀请应答表</p>
	保密方案	<p>供应商提供针对本项目的保密方案，内容包括：①保密管理制度；②针对本项目的保密措施。一、评审标准（1）针对性：每项方案能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性：每项方案内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。二、赋分标准(满分4分)共2项内容，每项满分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>商务应答表</p> <p>服务方案</p> <p>服务内容及服务邀请应答表</p> <p>保密方案（包二）.docx</p>

企业实力	<p>针对本项目的供应商实力说明，内容包含：①数据安全保障支撑能力，具备国家权威机构颁发的信息安全服务资质-数据安全类资质；②供应商自身安全保障能力，具备GB/T40753或ISO/IEC28000供应链安全管理体系认证；③持续安全运营服务能力，具备国家权威机构颁发的信息安全服务资质-安全运营类资质；④具备GB/T22080或ISO/IEC27000信息安全管理体系认证。</p> <p>一、评审标准：提供相关证明材料，如国家权威机构体系认证证书复印件及信息查询截图证明并盖章，得1分，未提供得0分。此项最高得分1分。二、赋分标准（满分4分），共4项内容，每项满分1分。按照“评审标准”，每个每满足1个评审标准得1分，未提供得0分。</p>	4.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包二）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	<p>供应商必须针对本项目组建专项技术服务团队，项目经理1人，驻场服务人员不少于16人并提供驻场人员一致性承诺，驻场不足16人或未提供承诺不得分，在满足人员要求基础上进行以下赋分：1、项目经理：①具有中级及以上信息安全工程师职称资格证书；②注册应急响应工程师CISP-IRE或注册应急响应专家CISP-IRS或注册威胁响应工程师CISP-TRE或注册威胁响应专家CISP-TRS或网络安全应急响应工程师CSERE或网络安全能力认证（CSC）任意一项证书。2、驻场运营团队：供应商针对本项目组建专项技术服务团队（除项目经理外）不少于16人，其中①具备注册信息安全工程师（CISP）不少于7人；②具备独立漏洞挖掘及发现能力（CNVD国家信息安全漏洞共享平台原创漏洞证明）不少于3人；③具备CISAW信息安全保障人员-安全</p>			

团队力量	<p>运维资质不少于1人；④具备注册信息安全讲师资质CISP-CISI不少于1人；⑤具备云安全工程师CISP-CSE不少于2人；⑥具备注册应急响应工程师CISP-IRE或注册应急响应专家CISP-IRS或注册威胁响应工程师CISP-TRE或注册威胁响应专家CISP-TRS或网络安全应急响应工程师CSERE或网络安全能力认证（CSC）不少于2人。一、评审标准：所有证书不得为协会类证书，按要求提供相关证明材料如证书复印件及国家权威机构对个人证书的信息查询截图证明并加盖公章。（1）项目经理1人，提供中级信息安全工程师证明得2分，提供应急响应证书得1分，未提供得0分。此项最高得分3分。（2）驻场运营团队不少于16人，提供资质不得同一人员重复使用，每提供一项资质得0.5分，未提供得0分。此项最高得分8分。二、赋分标准（满分11分），共2项，项目经理项满分3分，驻场运营团队项满分8分。按照“评审标准”，项目经理满足中级信息安全工程师要求得2分，提供应急响应类证书得1分，未提供得0分；驻场运营团队项目每满足一个评审标准得0.5分，未提供得0分。备注：需提供有效的证书复印件。</p>	11.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包二）.docx</p> <p>商务应答表</p> <p>服务方案</p>
------	---	---------	----	---

	团队组织架构	<p>供应商提供针对本项目拟投入的项目团队成员的情况说明。内容至少包含：①团队成员管理组织架构、人员分工;②项目工作职责划分、项目管理流程等内容。 一、评审标准：（1）针对性:内容能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。 二、赋分标准（满分2分），共2项内容，每项最高得1分。按照“评审标准”，每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包二）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	业绩	<p>供应商需提供2022年01月01日（日期以签订合同实际为准）至今，承接的同类（信息安全服务类）项目的业绩经验。提供采购合同复印件并加盖供应商公章。不满足要求不得分。 一、评审标准：每提供一份证明材料得1分，未提供得0分，此项最高5分。 二、赋分标准（满分5分）共1项内容，满分5分。按照“评审标准”每满足一个评审标准得1分，未提供得0分。</p>	5.0000	客观	<p>商务应答表</p> <p>服务方案</p> <p>业绩（包二）.docx</p>
价格分	价格分	<p>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.符合招标文件规定的小微企业、监狱企业、残疾人福利性单位优惠条件的供应商，价格给予10%的扣除，用扣除后的价格参与评审。 5.明显低于成本价进行报价的投标视为无效投标。</p>	10.0000	客观	<p>投标函</p> <p>分项报价表（包二）.docx</p> <p>开标一览表</p> <p>标的清单</p>

价格扣除

序号	价格扣除评审内容	适用情形	扣除比例 (C1)	具体标准和要求	关联投标（响应）文件 格式文件
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

采购包3:

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

	现状及需求分析	<p>供应商提供针对本项目现状及需求分析，内容包含：①对陕西省数字政府终端行为分析服务需求及现状的理解；②对本项目的业务现状分析；③对本项目业务需求分析。一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分12分）共3项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 现状及需求分析（包三）.docx
	服务要求响应方案	<p>供应商依据招标人所提供对本项目的①终端行为分析服务；②终端合规监控服务等2项服务要求进行实质性响应并进行优化提升的。一、评审标准（1）专业性：切合本项目实际情况，提出专业性强、科学合理的方案得2分，有缺陷得1分，未提供得0分。（2）可实施性：切合本项目实际情况，提出步骤清晰、专业性强、合理的方案得2分，有缺陷得1分，未提供得0分。（3）针对性：方案能够紧扣项目实际需求，内容科学，保障项目顺利实施得2分，有缺陷得1分，未提供得0分。此项最高得分6分。二、赋分标准（满分12分），共2项，每项满分6分。按照“评审标准”，每个方案每满足一项评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表 服务要求响应方案（包三）.docx

服务方案	<p>供应商提供针对本项目的服务方案，方案包含：①服务内容；②服务频次；③服务工具（部署、保障、功能证明材料等）；④服务成果。</p> <p>一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分16分）共4项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	16.0000	主观	<p>服务内容及服务邀请应答表</p> <p>商务应答表</p> <p>服务方案</p>
服务保证措施	<p>供应商提供针对本项目的服务保证措施，内容包括：①质量保证措施；②进度保证措施；③组织保障措施；④项目管理措施；⑤风险处置措施。一、评审标准（1）针对性：每项方案能够紧扣项目实际情况得2分，有缺陷得1分，未提供得0分。（2）合理性：每项方案内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分20分）共5项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	20.0000	主观	<p>服务内容及服务邀请应答表</p> <p>服务保证措施（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>

详细评审	保密方案	<p>供应商提供针对本项目的保密方案，内容包括:①保密管理制度:②针对本项目的保密措施。一、评审标准（1）针对性:方案能够紧扣项目实际情况，得2分，有缺陷得1分，未提供得0分。（2）合理性:内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准(满分8分)共2项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	8.0000	主观	<p>服务内容及服务邀请应答表</p> <p>保密方案（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	企业实力	<p>针对本项目的供应商实力说明，内容包括：①具备GB/T22080或ISO 27000信息安全管理体认证证书；②供应商具备信息安全服务资质认证证书。一、评审标准：提供相关证明材料，如国家权威机构体系认证证书复印件及信息查询截图证明并盖章，得2分，未提供得0分。此项最高得分4分。二、赋分标准（满分4分）共2项内容，每项最高2分。按照“评审标准”，每个每满足1个评审标准得2分，未提供得0分。</p>	4.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>

团队力量	<p>供应商必须针对本项目组建专项技术服务团队，投入项目的总服务人员不少于5人，需提供每周1人/天驻场服务提供终端安全风险处置服务。在满足人员要求基础上进行以下赋分： 1、项目经理：①具有信息化类中级及以上工程师职称资格证书；②具有注册信息安全工程师证书(CISP)。 2、团队人员（除项目经理外）不少于4人。①具有信息化类中级工程师职称资质证书；②具有注册信息安全工程师证书(CISP)。 一、评审标准：所有证书不得为协会类证书，按要求提供相关证明材料如证书复印件及国家权威机构对个人证书的信息查询截图证明并加盖公章。（1）项目经理1人，每提供一项资质得2分，未提供得0分。此项最高得分4分。（2）团队人员不少于4人，提供资质不得同一人员重复使用，每提供一项资质得1分，未提供得0分。此项最高得分4分。 二、赋分标准（满分8分），共2项，项目经理项满分4分，团队人员满分4分。按照“评审标准”，项目经理每满足一个评审标准得2分，未提供得0分。团队人员每满足一个评审标准得1分，未提供得0分。 备注：需提供有效的证书复印件。</p>	8.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>
------	--	--------	----	---

	团队组织架构	<p>供应商提供针对本项目拟投入的工作组成员的情况说明。内容至少包含：①工作组成员管理组织架构、人员分工;②工作职责划分、业务管理流程等内容。 一、评审标准（1）针对性:内容能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。 二、赋分标准(满分2分)共2项内容，每项满分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	业绩	<p>供应商需提供2022年01月01日（日期以签订合同实际为准）至今，承接的同类（信息化运维类）项目的业绩经验。提供采购合同复印件并加盖供应商公章。不满足要求不得分。 一、评审标准：每提供一份证明材料得2分，未提供得0分，此项最高得分8分。 二、赋分标准（满分8分）共1项内容，满分8分。按照“评审标准”每满足一个评审标准得2分，未提供得0分。</p>	8.0000	客观	<p>业绩（包三）.docx</p> <p>商务应答表</p> <p>服务方案</p>
价格分	价格分	<p>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）$\times 10$的公式计算得分，计算分数时四舍五入取小数点后两位。 4.符合招标文件规定的小微企业、监狱企业、残疾人福利性单位优惠条件的供应商，价格给予10%的扣除，用扣除后的价格参与评审。 5.明显低于成本价进行报价的投标视为无效投标。</p>	10.0000	客观	<p>开标一览表</p> <p>标的清单</p> <p>投标函</p> <p>分项报价表（包三）.docx</p>

价格扣除

序号	价格扣除评审内容	适用情形	扣除比例 (C1)	具体标准和要求	关联投标（响应）文件格式文件
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

采购包4:

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

	现状及需求分析	<p>供应商提供针对本项目现状及需求分析，内容包含：①对陕西省数字政府网络和数据安全风险评服务需求及现状的理解；②对本项目的业务现状分析；③对本项目业务需求分析。一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分12分）共3项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	客观	<p>服务内容及服务邀请应答表</p> <p>现状及需求分析（包四）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	服务要求响应方案	<p>供应商依据招标人所提供对本项目的①网络安全风险评估服务；②数据安全管理服务（数据安全风险评估），等2项服务要求进行实质性响应并进行优化提升的。一、评审标准（1）专业性：方案切合本项目实际情况，提出专业性强、科学合理得2分，有缺陷得1分，未提供得0分。（2）可实施性：方案切合本项目实际情况，步骤清晰、专业性强、合理得2分，有缺陷得1分，未提供得0分。（3）针对性：方案能够紧扣项目实际需求，内容科学，保障项目顺利实施得2分，有缺陷得1分，未提供得0分。此项最高得分6分。二、赋分标准（满分12分），共2项，每项满分6分。按照“评审标准”，每个每满足一项评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	<p>服务内容及服务邀请应答表</p> <p>服务要求响应方案（包四）.docx</p> <p>商务应答表</p> <p>服务方案</p>

服务方案	<p>供应商提供针对本项目的服务方案，方案包含：①服务内容；②服务频次；③服务成果。一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：方案内容符合项目实际，未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。</p> <p>二、赋分标准（满分12分）共3项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	<p>服务内容及服务邀请应答表</p> <p>商务应答表</p> <p>服务方案</p>
服务保证措施	<p>供应商提供针对本项目的服务保证措施，内容包括：①质量保证措施；②进度保证措施；③组织保障措施；④项目管理措施；⑤风险控制措施。一、评审标准（1）针对性：方案能够紧扣项目实际情况得2分，有缺陷得1分，未提供得0分。（2）合理性：方案内容符合项目实际，未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分20分）共5项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	20.0000	主观	<p>服务内容及服务邀请应答表</p> <p>商务应答表</p> <p>服务方案</p> <p>服务保证措施（包四）.docx</p>

详细评审

保密方案	供应商提供针对本项目的保密方案，内容包括:①保密管理制度:②针对本项目的保密措施。一、评审标准（1）针对性:方案能够紧扣项目实际情况，得2分，有缺陷得1分，未提供得0分。（2）合理性:方案内容符合项目实际，未出现与项目执行无关内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准(满分8分)共2项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分	8.0000	主观	服务内容及服务邀请 应答表 保密方案（包四）.docx 商务应答表 服务方案
企业实力	供应商提供服务能力证明：①具备GB/T22080或ISO/IEC27000信息安全管理体系认证证书；②具备信息安全风险评估服务资质证书。一、评审标准：提供相关证明材料，如国家权威机构体系认证证书复印件及信息查询截图证明并盖章，得2分，未提供得0分。此项最高得分4分。二、赋分标准（满分4分），共2项内容，每项最高2分。按照“评审标准”，每个每满足1个评审标准得2分，未提供得0分。	4.0000	客观	商务应答表 服务方案 服务内容及服务邀请 应答表 项目人员及供应商认为有必要补充说明的其他内容（包四）.docx

团队力量	<p>供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于7人，现场驻场服务人员不少于1人。在满足人员要求基础上进行以下赋分： 1、项目经理：①具有中级及以上信息安全工程师职称资格证书；②具有注册信息安全工程师证书(CISP)。 2、团队人员（除项目经理外）：服务人员具有注册信息安全工程师证书(CISP)。</p> <p>一、评审标准：所有证书不得为协会类证书，按要求提供相关证明材料如证书复印件及国家权威机构对个人证书的信息查询截图证明并加盖公章。（1）项目经理1人，提供工程师职称资格证书得2分，提供注册信息安全工程师证书得2分，未提供得0分。此项最高得分4分。</p> <p>（2）团队人员（除项目经理外）不少于6人，提供资质不得同一人员重复使用，每提供一项资质得1分，未提供得0分。此项最高得分6分。 二、赋分标准（满分10分），共2项，项目经理满分4分，团队人员满分6分。按照“评审标准”，项目经理工程师职称资格得2分，注册信息安全工程师证书2分。团队人员每满足一个评审标准得1分，未提供得0分。 备注：需提供有效的证书复印件。</p>	10.0000	客观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包四）.docx</p> <p>商务应答表</p> <p>服务方案</p>
------	---	---------	----	---

	团队组织架构	<p>供应商提供针对本项目拟投入的工作组成员的情况说明。内容至少包含：①工作组成员管理组织架构、人员分工;②工作职责划分、业务管理流程等内容。 一、评审标准（1）针对性:内容能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分1分。 二、赋分标准(满分2分)共2项内容，每项满分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包四）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	业绩	<p>供应商需提供2022年01月01日（日期以签订合同实际为准）至今，承接的同类（风险评估服务类）项目的业绩经验。提供采购合同复印件并加盖供应商公章。不满足要求不得分。 一、评审标准：每提供一份证明材料得2分，未提供得0分，此项最高得分10分。 二、赋分标准（满分10分）共1项内容，满分10分。按照“评审标准”每满足一个评审标准得2分，未提供得0分。</p>	10.0000	客观	<p>业绩（包四）.docx</p> <p>商务应答表</p> <p>服务方案</p>
价格分	价格分	<p>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）$\times 10$的公式计算得分，计算分数时四舍五入取小数点后两位。 4.符合招标文件规定的小微企业、监狱企业、残疾人福利性单位优惠条件的供应商，价格给予10%的扣除，用扣除后的价格参与评审。 5.明显低于成本价进行报价的投标视为无效投标。</p>	10.0000	客观	<p>投标函</p> <p>分项报价表（包四）.docx</p> <p>开标一览表</p> <p>标的清单</p>

价格扣除

序号	价格扣除评审内容	适用情形	扣除比例 (C1)	具体标准和要求	关联投标（响应）文件格式文件
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

采购包5:

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

	现状及需求分析	<p>供应商提供针对本项目现状及需求分析，内容包含：①对陕西省数字政府网络安全测试服务现状及需求的理解；②对本项目的业务现状分析；③对本项目业务需求分析。一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：内容符合项目实际、未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分12分）共3项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	<p>服务内容及服务邀请应答表</p> <p>现状及需求分析（包五）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	服务要求响应方案	<p>供应商依据招标人所提供对本项目的①渗透测试服务；②源代码安全审计服务，等2项服务要求进行实质性响应并进行优化提升的。一、评审标准（1）专业性：方案切合本项目实际情况，提出专业性强、科学合理得2分，有缺陷得1分，未提供得0分。（2）可实施性：方案切合本项目实际情况，步骤清晰、专业性强、合理得2分，有缺陷得1分，未提供得0分。（3）针对性：方案能够紧扣项目实际需求，内容科学，保障项目顺利实施得2分，有缺陷得1分，未提供得0分。此项最高得分6分。二、赋分标准（满分12分），共2项，每项满分6分。按照“评审标准”，每个每满足一项评审标准得2分，有缺陷得1分，未提供得0分。</p>	12.0000	主观	<p>服务内容及服务邀请应答表</p> <p>服务要求响应方案（包五）.docx</p> <p>商务应答表</p> <p>服务方案</p>

服务方案	<p>供应商提供针对本项目的服务方案，方案包含：①服务内容；②服务频次；③服务工具（部署、保障、功能证明材料等）；④服务成果。</p> <p>一、评审标准：（1）针对性：方案能够紧扣项目情况得2分，有缺陷得1分，未提供得0分。（2）合理性：方案内容符合项目实际，未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分16分）共4项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	16.0000	主观	商务应答表 服务方案 服务内容及服务邀请 应答表
服务保证措施	<p>供应商提供针对本项目的服务保证措施，内容包括：①质量保证措施；②进度保证措施；③组织保障措施；④项目管理措施；⑤风险控制措施。一、评审标准（1）针对性：方案能够紧扣项目实际情况得2分，有缺陷得1分，未提供得0分。（2）合理性：方案内容符合项目实际，未出现与项目执行无关的内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准（满分20分）共5项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	20.0000	主观	服务内容及服务邀请 应答表 服务保证措施（包五）.docx 商务应答表 服务方案

详细评审	保密方案	<p>供应商提供针对本项目的保密方案，内容包括:①保密管理制度:②针对本项目的保密措施。一、评审标准（1）针对性:方案能够紧扣项目实际情况，得2分，有缺陷得1分，未提供得0分。（2）合理性:方案内容符合项目实际，未出现与项目执行无关内容得2分，有缺陷得1分，未提供得0分。此项最高得分4分。二、赋分标准(满分8分)共2项内容，每项满分4分。按照“评审标准”，每个每满足一个评审标准得2分，有缺陷得1分，未提供得0分。</p>	8.0000	主观	<p>服务内容及服务邀请应答表 保密方案（包五）.docx 商务应答表 服务方案</p>
	企业实力	<p>供应商提供具备能力的资质证明，供应商具备信息安全服务资质证书，网络安全审计服务资质或软件安全测试服务资质证书之一。一、评审标准：提供相关证明材料，如国家权威机构体系认证证书复印件及信息查询截图证明并盖章，得2分，未提供得0分。此项最高得分4分。二、赋分标准：共2项内容，每项最高2分，满分4分。按照“评审标准”，每满足1个评审标准得2分，未提供得0分。</p>	4.0000	客观	<p>服务内容及服务邀请应答表 项目人员及供应商认为有必要补充说明的其他内容（包五）.docx 商务应答表 服务方案</p>

团队力量	<p>供应商必须针对本项目组建专项技术服务团队，投入项目的服务人员不少于13人，提供驻场测试服务人员不少于2人。在满足人员要求基础上进行以下赋分：1、项目经理：①具有中级及以上信息安全工程师职称资格证书；②注册信息安全工程师证书(CISP)。2、团队人员（除项目经理外）：服务人员注册信息安全工程师证书(CISP)不少于2人，注册渗透测试工程师CISP-PTE或专家证书CISP-PTS不少于4人。</p> <p>一、评审标准：所有证书不得为协会类证书，按要求提供相关证明材料如证书复印件及国家权威机构对个人证书的信息查询截图证明并加盖公章。（1）项目经理1人，提供信息安全工程师职称资格证书得1分，提供注册信息安全工程师证书得1分，未提供得0分。此项最高得分2分。（2）团队人员不少于12人，提供资质不得同一人员重复使用，每提供一项资质得1分，未提供得0分。此项最高得分6分。</p> <p>二、赋分标准（满分8分），共2项，项目经理满分2分，团队人员满分6分。按照“评审标准”，项目经理工程师职称资格得1分，注册信息安全工程师证书1分。团队人员每满足一个评审标准得1分，未提供得0分。备注：需提供有效的证书复印件。</p>	8.0000	客观	<p>商务应答表</p> <p>服务方案</p> <p>服务内容及服务邀请</p> <p>应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包五）.docx</p>
------	---	--------	----	---

	团队组织架构	<p>供应商提供针对本项目拟投入的工作组成员的情况说明。内容至少包含：①工作组成员管理组织架构、人员分工;②工作职责划分、业务管理流程等内容。 一、评审标准（1）针对性:内容能够紧扣项目实际情况，得0.5分，未提供得0分。（2）合理性:内容符合项目实际，未出现与项目执行无关的内容，得0.5分，未提供得0分。此项最高得分2分。 二、赋分标准(满分2分)共2项内容，每项满分1分。按照“评审标准”，每个每满足一个评审标准得0.5分，未提供得0分。</p>	2.0000	主观	<p>服务内容及服务邀请应答表</p> <p>项目人员及供应商认为有必要补充说明的其他内容（包五）.docx</p> <p>商务应答表</p> <p>服务方案</p>
	业绩	<p>供应商需提供2022年01月01日（日期以签订合同实际为准）至今，承接的同类（安全测试类）项目的业绩经验。提供采购合同复印件并加盖供应商公章。不满足要求不得分。 一、评审标准：每提供一份证明材料得2分，未提供得0分，此项最高8分。 二、赋分标准（满分8分）共1项内容。按照“评审标准”每满足一个评审标准得2分，未提供得0分。</p>	8.0000	客观	<p>商务应答表</p> <p>服务方案</p> <p>业绩（包五）.docx</p>
价格分	价格分	<p>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）$\times 10$的公式计算得分，计算分数时四舍五入取小数点后两位。 4.符合招标文件规定的小微企业、监狱企业、残疾人福利性单位优惠条件的供应商，价格给予10%的扣除，用扣除后的价格参与评审。 5.明显低于成本价进行报价的投标视为无效投标。</p>	10.0000	客观	<p>投标函</p> <p>分项报价表（包五）.docx</p> <p>开标一览表</p> <p>标的清单</p>

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 文件格式文件
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 标的清单 中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件

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：保密方案（包一）.docx

详见附件：非联合体承诺书（包一）.docx

详见附件：分项报价表（包一）.docx

详见附件：服务保证措施（包一）.docx

详见附件：服务要求响应方案（包一）.docx

详见附件：供应商关联承诺书（包一）.docx

详见附件：拒绝政府采购领域商业贿赂承诺书（包一）.docx

详见附件：培训方案（包一）.docx

详见附件：现状及需求分析（包一）.docx

详见附件：项目人员及供应商认为有必要补充说明的其他内容（包一）.docx

详见附件：业绩（包一）.docx

详见附件：资格证明文件（包一）.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：保密方案（包二）.docx

详见附件：非联合体承诺书（包二）.docx

详见附件：分项报价表（包二）.docx

详见附件：服务保证措施（包二）.docx

详见附件：服务要求响应方案（包二）.docx

详见附件：供应商关联承诺书（包二）.docx

详见附件：拒绝政府采购领域商业贿赂承诺书（包二）.docx

详见附件：现状及需求分析（包二）.docx

详见附件：项目人员及供应商认为有必要补充说明的其他内容（包二）.docx

详见附件：业绩（包二）.docx

详见附件：资格证明文件（包二）.docx

采购包3：

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：保密方案（包三）.docx

详见附件：非联合体承诺书（包三）.docx

详见附件：分项报价表（包三）.docx

详见附件：服务保证措施（包三）.docx

详见附件：服务要求响应方案（包三）.docx

详见附件：供应商关联承诺书（包三）.docx

详见附件：拒绝政府采购领域商业贿赂承诺书（包三）.docx

详见附件：现状及需求分析（包三）.docx

详见附件：项目人员及供应商认为有必要补充说明的其他内容（包三）.docx

详见附件：业绩（包三）.docx

详见附件：资格证明文件（包三）.docx

采购包4：

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：保密方案（包四）.docx

详见附件：非联合体承诺书（包四）.docx

详见附件：服务保证措施（包四）.docx

详见附件：服务要求响应方案（包四）.docx

详见附件：供应商关联承诺书（包四）.docx

详见附件：拒绝政府采购领域商业贿赂承诺书（包四）.docx

详见附件：现状及需求分析（包四）.docx

详见附件：项目人员及供应商认为有必要补充说明的其他内容（包四）.docx

详见附件：业绩（包四）.docx

详见附件：资格证明文件（包四）.docx

详见附件：分项报价表（包四）.docx

采购包5:

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：保密方案（包五）.docx

详见附件：非联合体承诺书（包五）.docx

详见附件：分项报价表（包五）.docx

详见附件：服务保证措施（包五）.docx

详见附件：服务要求响应方案（包五）.docx

详见附件：供应商关联承诺书（包五）.docx

详见附件：拒绝政府采购领域商业贿赂承诺书（包五）.docx

详见附件：现状及需求分析（包五）.docx

详见附件：项目人员及供应商认为有必要补充说明的其他内容（包五）.docx

详见附件：业绩（包五）.docx

详见附件：资格证明文件（包五）.docx

第7章 拟签订采购合同文本

详见附件：附件：合同.docx

