周口市公共资源交易中心

政 府 采 购 招 标 文 件

2 包

项目名称：周口日报社国产化机房政务云改造项目

项目编号：周财招标采购-2025-10

2025 年 2 月

目　录

第一章　招标公告

项目概况

周口日报社国产化机房政务云改造项目的潜在投标人应在周口市公共资源交易中心网（ http://jyzx.zhoukou.gov.cn）获取招标文件，并于 2025 年 3 月 3 日 10 点 00 分（北京时间）前递交投标文件。

一、项目基本情况

项目编号：周财招标采购-2025-10

项目名称：周口日报社国产化机房政务云改造项目

预算金额：6102041.00 元

最高限价（如有）：6102041.00 元

采购方式：公开招标

包别划分：2 个包

包号	包名称	包最高限价元
1	周口日报社国产化机房政务云改造项目 1 包	6102040.00
2	周口日报社国产化机房政务云改造项目 2 包	1.00

采购需求：

1包：服务器升级改造、网络系统升级改造、存储系统升级改造、云化软件等软硬件采购。(详见招标文件)

2包：云安全资源池和云密码资源池服务。(详见招标文件)

合同履行期限：1包：合同签订后90日历天内供货安装调试完成。

2包：3年

是否接受进口产品：否

本项目是否接受联合体投标：否

本项目是否为只面向中小企业采购：否

二、申请人的资格要求

1.满足《中华人民共和国政府采购法》第二十二条规定；

（1）具有独立承担民事责任的能力（企业营业执照等证明文件）；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录（缴纳的税收凭据、社会保险凭据，依法免税或不需要缴纳社会保障资金的供应商应提供相应的证明文件）；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供没有重大违法记录的书面声明函，格式自拟）；

2.落实政府采购政策需满足的资格要求：促进中小企业和监狱企业发展扶持政策、政府强制采购节能产品强制采购、节能产品及环境标志产品优先采购、促进残疾人就业政府采购政策。

3.本项目的特定资格要求：

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)和豫财购【2016】15号的规定，对列入“信用中国”网站（www.creditchina.gov.cn）的“失信被执行人”、“重大税收违法案件当事人名单（重大税收违法失信主体）”和“中国政府采购”网站(www.ccgp.gov.cn)的“政府采购严重违法失信行为记录名单”的供应商，将拒绝其参加政府采购活动；在标书中附加盖公章的网页查询扫描件，查询日期为公告发布之日起至投标截止之日止。

三、获取招标文件

时间：2025年2月10日至2025年2月17日 ，每天上午0：00至12:00，下午12:00至23:59（北京时间，法定节假日除外）

地点：周口市公共资源交易中心网（http://jyzx.zhoukou.gov.cn）

方式：供应商请在网站自主注册后下载采购文件（zkzf格式）及资料，需办理CA数字证书后方可提交响应文件，具体办理事宜请查阅周口市公共资源交易中心网站。

售价：0 元

四、提交投标文件截止时间、开标时间和地点

时间：2025 年 3 月 3 日 10 点 00 分（北京时间）

地点：周口市公共资源交易中心网（http://jyzx.zhoukou.gov.cn）

五、公告期限

本次招标公告在《河南省政府采购网》《周口市公共资源交易中心网》上发布，招标公告期限为 5 个工作日。

六、其他补充事宜

无

七、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名称：周口日报社

地址：周口市周口大道中段 6 号

项目联系人：张峰　　联系方式：0394-6193305

2.采购代理机构信息

名称：周口市公共资源交易中心政府采购中心

地址：周口市光明路与政通路交叉口向北 100 米路东

项目联系人：刘宇　　联系方式：0394-8106517

3.监督单位：周口市财政局政府采购监督管理科

联系方式： 0394-8319709

周口市公共资源交易中心政府采购中心

2025 年 2 月 10 日

第二章 投标人须知前附表

序号	内容	说明与要求
1	采购人	周口日报社
2	委托人	周口日报社
3	采购代理机构	名　称：周口市公共资源交易中心政府采购中心 地　址：周口市光明路与政通路交叉口向北 100 米路东
4	项目名称	周口日报社国产化机房政务云改造项目
5	项目编号	周财招标采购-2025-10
6	项目性质	2 包：服务类；
7	资金来源	自筹资金
8	包别划分	本次招标共分 2 个包： 2 包：云安全资源池和云密码资源池服务。
9	付款方式	2 包：服务通过验收后，根据实际使用量结算，最终客户结算款*折扣率结算服务费，每一年结算一次。 提醒:请采购人按照相关文件要求对本次采购活动填写详细支付方式。(本次政府采购活动鼓励采购人在政府采购合同中约定预付款，原则上预付款比例不低于合同金额的 40%，对于中小企业的预付款比例不低于合同金额的 60%。采购人可根据项目特点、供应商信用情况等，要求供应商应提供预付款保函或其他非现金担保。政府采购项目预付款应在合同备案通过、具备约定支付条件后 3 个工作日内完成支付。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，预付款从其有关规定执行。 对于未实行预付款的政府采购项目鼓励采购人在合同中明确首付款支付比例。原则上首付款支付比例不低于合同金额的 50%;对于中小企业的首付款支付比例不低于合同金额的 70%。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，首付款从其有关规定执行)。
10	联合体投标	不允许
11	投标有效期	开标后 60 天
12	服务地点	采购人指定地点
13	合同履行期限	3 年
14	投标保证金金额	不需要缴纳投标保证金（按照相关文件要求货物、服务类政府采购活动不收取投标保证金、履约、质量保证金、合同中预留资金作为质量保证金等无法律依据的保证金。政府采购工程推广以承诺书替代保证金，投标人应提供投标承诺函。）。

15	答疑	疑问的提出与答疑获取详见招标文件第二部分第五章投标人须知第36条。 周口市公共资源交易中心政府采购中心对招标文件进行的澄清、更正或更改，将在网站上及时发布，该公告内容为招标文件的组成部分，对投标人具有同样约束力效力。投标人应主动上网查询。周口市公共资源交易中心政府采购中心不承担投标人未及时关注相关信息引发的相关责任。
16	勘察现场	本项目需要勘察现场，各投标人于招标公告截止后的第一个工作日进行现场勘察，并由采购人出具加盖公章的勘察证明。
17	投标文件	1、投标文件为使用周口市公共资源交易中心提供的电子标书制作工具软件（http://jyzx.zhoukou.gov.cn 网上下载）制作生成的电子加密文件，应在投标截止时间前通过周口市公共资源交易中心会员系统上传。投标截止时间前不上传电子投标文件或者在开标时间不进行电子投标文件解密，均视为自动放弃投标。 2、本项目实行网上远程开标无须到现场提交响应文件，未加密的电子投标文件和纸质文件不再提交。
18	投标时间及地点	投标截止时间：***年***月***日（见招标公告） 标书递交地点：周口市公共资源交易中心网 网址：周口市公共资源电子交易服务平台会员系统（网址http://jyzx.zhoukou.gov.cn） （本项目实行网上远程开标无须到现场提交响应文件）
19	开标时间及地点	开标时间：***年***月***日（见招标公告） 开标地点：周口市东新区光明路市行政中心西侧南楼房间（本项目实行网上远程开标无须到现场提交响应文件）
20	评标办法	综合评分法 详见招标文件第一部分第四章评标办法
21	所属行业类别	软件和信息技术服务业。
22	报价说明	本项目不进行报价，招标文件中凡涉及报价的条款可忽略，但基于河南省政府采购系统预算金额为必填项，本次采购预算金额设定为“1元”，此预算金额不作为报价依据。供应商在递交投标文件时，电子系统涉及的报价必填项可填写“1元”，此项不作为废标或得分的依据。
23	其它	采购人验收如需第三方质检部门介入，第三方质检验收所需费用由中标人负担。

第三章　需求一览表

前注：1） 本需求中提出的技术方案仅为参考，如无明确限制，投标人可以进行优化，提供满足用户实际需要的更优（或者性能实质上不低于的）技术方案或者设备配置，且此方案或配置须经评委会审核认可；

2） 为鼓励不同品牌的充分竞争，如某设备的某技术参数或要求属于个别品牌专有，则该技术参数及要求不具有限制性，投标人可对该参数或要求进行适当调整，并应当说明调整的理由，且此调整须经评委会审核认可；

3） 为有助于投标人选择投标产品，项目需求中提供了推荐品牌（或型号）、参考品牌（或型号）等，但这些品牌（或型号）仅供参考，并无限制性。投标人可以选择性能不低于推荐（或参考）的品牌（或型号）的其他品牌产品，但投标时应当提供有关技术证明资料，未提供的可能导致投标无效；

4）投标人应当在投标文件中列出完成本项目并通过验收所需的所有各项服务等明细表及全部费用。中标人必须确保整体通过用户方及有关主管部门验收，所发生的验收费用由中标人承担；投标人应自行踏勘现场，如投标人因未及时踏勘现场而导致的报价缺项漏项废标、或中标后无法完工，投标人自行承担一切后果；

5）如对本招标文件有任何疑问或澄清要求，请按本招标文件“投标人须知前附表”中约定联系周口市公共交资源交易中心政府采购中心，或接受答疑截止时间前联系采购人。否则视同理解和接受。

服务需求

云安全资源池和云密码资源池服务需求

（一）项目背景

周口日报社国产化政务云分为互联网区与政务外网区，按照等级保护三级的基本要求进行总体规划和设计；本次建设的国产化政务云安全资源池和云密码资源池主要为云租户的业务系统提供网络安全服务和商业密码应用服务，满足业务系统信息安全等级保护和商用密码应用安全性评估的要求。为保障云租户的业务系统运行安全、提供云租户全面服务能力及弹性扩展安全能力；建设周口日报社国产化政务云云安全资源池、云密码资源池，满足云租户业务系统上云合规要求及业务生命周期内的安全需求。

（二）建设内容

1、本项目包含云安全资源池支撑硬件、云安全管理平台、云密码资源池支撑硬件、密码服务平台等所涉及的软硬件设备及安装部署，同时包含软件升级、远程技术支持和驻场运维服务。

2、云安全资源池须包括 8 类及以上安全服务能力，包括且不限于以下服务：入侵检测服务、WEB 应用防火墙服务、漏洞扫描服务、网页防篡改服务、堡垒机服务、主机杀毒服务、日志审计服务、数据库审计服务等。

3、云密码资源池须包括 10 类及以上密码服务能力，包括且不限于以下服务：密钥管理服务、加解密服务、签名验签服务、SSL VPN 接入服务、IPSEC VPN 服务、时间戳服务、安全认证服务、协同签名服务、数据库加密服务、文件加密服务等。

（三）功能要求

网络情况分为周口日报社国产化政务云互联网区、政务云政务外网区；周口大数据中心政务云互联网区、政务云政务外网区，每个区都有单独的出口。

1、安全资源池和密码资源池需求：分别为周口日报社国产化政务云互联网区、政务云政务外网区、周口大数据中心政务云互联网区和政务云政务外网区四个区域提供安全和密码服务，安全资源池和密码资源池需要满足三年内各委办局不断增加业务系统的需要，基于各委办局单位建立单独的运维管理账号，云租户单位能独立管理所需的安全和密码服务组件。

2、当云安全资源池和云密码资源池资源不能满足政务云的需要，投标人应按实际需求及时进行扩容，提出需求后，15 天内满足服务要求，云安全资源池和云密码资源池在服务期内免费升级扩容。

3、投标人提供安全资源池、密码资源池建设所需要的软硬件设备（服务器、交换机、云服务器密码机、综合网关、云安全管理平台、密码服务平台、相关配件等）。

4、云安全资源池硬件、云安全管理平台、云密码资源池支持硬件、密码服务平台等所涉及的软硬件设备在招标人指定的机房内部署。

5、云安全资源池和云密码资源池需要提供各租户的服务使用情况明细报表，需要包含使用项目、使用时长、开启时间、结束时间、服务状态等信息。

6、需根据要求与省平台进行对接。

7、服务能力要求

（1）安全资源服务能力

服务项目	规　格	最小单位
★入侵检测服务	为云上系统提供南北向的网络层入侵检测服务，支持漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、暴力破解等的检测和防护，防护带宽≥50Mbps。	1IP
★WEB 应用防火墙服务	为云上 Web 应用系统提供应用层安全防护服务，支持 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护，http/https 协议防护带宽≥50Mbps。	1IP
★漏洞扫描服务	漏洞扫描系统，对云主机系统进行漏洞扫描，输出检测报告，提供修复建议。	1IP
★网页防篡改服务	实时监测和保护站点内容安全，防止非法篡改网页，保护站点公众形象。	1IP
★堡垒机服务	提供运维安全管理与审计系统，支持主机管理、权限控制、运维审计等功能。	1IP
★主机杀毒服务	提供主机杀毒功能，对云主机进行全面的病毒扫描、检测、清除和防护。	1 客户端
★日志审计服务	提供日志审计系统，对租户云主机、应用、网络设备等操作日志审计，支持日志采集、日志存储、日志检索、日志分析、可视化统计等。	1 日志源
★数据库审计服务	提供数据库审计系统，对数据库的操作行为审计 ，对各类数据库访问行为进行解析、分析、记录。	实例

（2）密码资源服务能力

服务项目	规　格	最小单位

★密钥管理服务	为租户提供密钥生成、存储、更新、备份、恢复及归档等密钥全生命周期管理。性能规格： 并发请求数≥100 次/秒， 密钥存储量>10000 个。	1 套
★加解密服务	提供标准 API 接口，为业务系统提供应用级数据加解密审杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护。性能规格： 并发请求数≥128 次/秒，SM1 计算速率≥15Mbps,SM2 加密≥2300 次/秒，SM2 解密≥1000 次/秒，SM4 计算速率≥150Mbps。	1 系统
★签名验签服务	基于数字签名、验证签名技术，为业务系统提供应用级数字签名、验证签名等服务。性能规格： 并发请求数≥128 次/秒，SM1 计算速率≥15Mbps,SM2 加密≥2300 次/秒，SM2 解密≥1000 次/秒，SM4 计算速率≥150Mbps。	1 系统
★SSL VPN 接入服务	面向运维侧为租户提供基于国密数字证书认证方式的安全接入，提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道(只提供账户服务，不包含数字证书及 USBkey)。	1 账户
★IPSEC VPN 服务	为租户提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道。性能规格：吞吐率≥500Mbps,最大并发隧道数≥1000 个。	1 套
★时间戳服务	提供时间戳签发、时间戳响应、时间戳解析、时间戳和有效性等多种安全功能。用于实现数据时间认证与签名需求奠定坚实基础。性能规格： 时间戳并发量≥100 个/秒，务信息管理局 时间戳签发≥80 次/秒，时间戳验证≥150 次/秒。	1 系统
★安全认证服务	为业务系统提供基于基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务。 性能规格：最大用户数≥500,加密吞吐量≥500Mbps	1 系统
★协同签名服务	用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥生成、密钥签名、密钥解密、密钥协同功能。性能规格： 身份认证≥1000 次/秒，并发速率≥1000,数字签名≥2000 次/秒，并发数≥100。	1 套
★数据库加密服务	提供数据库加密服务，实现对数据库关键字段或全库的数据进行加密保存，满足结构化数据的存储机密性及完整性要求。性能规格： SM4 的加密性能≥70Mbps, 数据库操作性能损耗≤20%, 加密性能≥5000QPS。	1 实例
★文件加密服务	提供非结构化文件加密服务，保障用户数据安全对非结构化文件提供加密服务，保障用户数据安全。性能规格： 文件读写操作性能损耗≤20%, 文件加密速率≥400Mbps。	1 系统

8、配套软硬件设施要求

序号	服务名称	配置说明

1	云安全资源池硬件	资源池硬件设施进行冗余，避免单点故障 1、资源池服务器 配置数量≥6 台 （1）国产化构架，2U 标准机架，双电源。 （2）CPU：国产化处理器≥48 核心*2 颗。 （3）内存：≥384G 内存。 （4）硬盘：系统盘≥960G SSD 服务器固态硬盘*2；缓存盘≥ 1.92T SSD 服务器固态硬盘*2；数据盘≥8T 服务器机械硬盘*8。 （5）接口：≥2 个千兆电口，≥4 个万兆光口。 2、引流交换机 配置数量≥4 台 （1）★交换容量≥4.8Tbps/96Tbps，包转发率≥2000Mpps； （2）端口要求：10GE 光端口数量≥48 个，固定 100GE 光接口≥6 个(兼容 40GE)。 （3）CPU 为国产自研芯片。 （4）L2 特性：支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术。 （5）L3 特性：支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议，支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。 （6）支持识别流量模型，动态调节 ECN 门限，支持无丢包缓存自动配置； （7）支持集群或堆叠多虚一技术，实现单一界面管理多台设备。 （8）支持 Vxlan，且支持 BGP EVPN 特性。 （9）★支持 openflow 技术。 （10）满配冗余电源、风扇。 （11）根据实际需要配备 100G 高速堆叠线缆，10G 光模块，40G 光模块。
2	云安全资源池管理平台	平台配置数量≥2 套 1、既支持独立资源池方式部署，又支持紧耦合方式部署。云安全管理平台和虚拟化安全设备部署在安全资源池内，安全资源池采用国产化服务器，与硬件设备的松耦合，无需专用硬件设备。虚拟化安全设备的容量可以随着国产化服务器数量的扩容而横向扩容。 2、云安全管理平台支持不同区域的多安全资源池统一平台管理（非不同管理页面跳转方式），用户可以选择在云主机对应的区域创建安全服务。 3、租户首页支持查看当前租户已经开通的安全组件和安全组件最近 7 天拦截的攻击数量和安全组件关联的资产的数量。 ★4、租户支持最少以 1 个资产起步开通、扩容、缩容入侵检测、WEB 应用防火墙、漏洞扫描、网页防篡改、堡垒机、主机杀毒、日志审计、数据库审计等安全能力组件。 5、支持安全组件批量开通，平台预置等保二级套餐、等保三级套餐。 6、支持在云安全管理平台管理页面查看数据库审计的审计资产信息，支持查看审计对象名称、数据库类型、版本、IP 地址、端口、应用规则组，支持对审计对象实现删除操作。 7、云安全管理平台支持华为 Cloudguard、华为 ManageOne、华为 MEC 管理平台、金山云、易捷行云、OpenStack、浪潮云、曙光云、华三云、移动咪咕云、Kylin、京东云、腾讯云、阿里云、中国电子云、优钛私有云、青云、云宏等主流云平台的对接。 8、支持在资产列表中查看资产对应的安全能力覆盖状态，支持显示资产的安全能力防护状态，支持为资产关联主机安全、边界安全、风险识别、日志审计、运维安全和网络威胁检测等安全能力。 9、支持监控全部物理资源和虚拟资源信息，除基本信息外，还展示单机实时服务状态、实时告警数量、实时 CPU/内存/磁盘使用率；支持按不同维度筛选和搜索；支持导出。 10、支持把组件日志、系统日志一起以 syslog 形式转发到指定的第三

		方日志服务器。支持安全日志以租户纬度和组件维度配置转发到不同的第三方服务器，同时支持原始日志转发和平台处理后的日志转发。 11、所投产品具备 CNNVD 或 CNVD 颁发的漏洞库兼容性资质证书，提供证书复印件。
3	安全资源池安全组件	1、云安全资源池至少支持部署入侵检测、WEB 应用防火墙、漏洞扫描、网页防篡改、堡垒机、主机杀毒、日志审计、数据库审计等安全组件进行安全防护、安全检测及安全运维。 2、支持对各类安全组件进行统一运维管理。 3、支持 VNC、单点登录方式连接安全组件，租户可从管理平台一键登录至安全组件 Web 配置界面。 4、支持安全组件配置一键导入导出、按周期定时导出。 5、支持自动下发 syslog 配置至各安全组件。 6、★支持安全组件的特征库通过云安全管理平台自动统一升级，且每个安全组件可以不需要连接互联网。 7、支持安全组件迁移，当资源池节点损坏时，安全组件可迁移至其他可用节点。 8、★支持租户/平台系统管理员纳管已有的安全组件(包括虚拟机、物理设备)并展示在安全组件列表中，可进行的操作包括登录、解除纳管。 9、★支持展示租户授权使用报表，展示安全组件授权使用情况，租户系统管理员可以导出授权使用报表，报表导出格式为 PDF。 10、支持链路聚合及端口绑定；支持 IPv6 网络；支持与第三方云平台的订单无缝对接。
4	云密码资源池硬件	**1、云服务器密码机：配置数量≥2 台** 1) 采用了密钥管理与设备管理分离的核心理念，实现了云应用环境下网络管理员仅维护设备，用户自行管理密钥的工作模式。云密码机通过密码机集群与虚拟化技术的结合扩充密码运算能力，将密码运算能力进行细粒度划分，并通过集中的密钥管理及配套的安全策略保护用户密钥整生命周期的安全。 2) 云服务器密码机支持基于 KVM 的虚拟化技术，在一个 CHSM 中虚拟出多个 VSM，内置支持 SR-IOV 虚拟化技术的硬件密码卡，提供密码模块的虚拟化支撑能力。 3) 云服务器密码机支持采用安全隔离技术，对每个 VSM 使用的密钥在存储和使用上进行了安全隔离。 4) ★云服务器密码机支持创建不同规格与性能的虚拟密码机；云服务器密码机支持利用负载均衡技术实现虚拟化实例对密码资源占用的分配，管理系统可以根据实际情况动态增加或释放密码运算资源。 5) 云服务器密码机支持 VLAN 池划分，当虚拟机选择同一个 VLAN 后，只同一个 VLAN 内的虚拟机可以互相访问，与其他虚拟机无法通信。 6) 云服务器密码机支持国密 SSH、国密 FTP，保证整机运维安全。 7) 云服务器密码机管理接口符合《云服务器密码机管理接口规范》的要求，可提供 CHSM 及 VSM 的配置管理接口。 8) 云服务器密码机支持多种国密算法，主要包括 SM1、SM2、SM3、SM4、等国密算法。 9) ★云服务器密码机支持虚拟机日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **2、服务器密码机：配置数量≥2 台** 1) 支持 SM1、SM2、SM3、SM4 国密算法。 2) 可提供对称算法加解密、非对称算法加密、解密、签名、验证，消息鉴别码产生与验证等密码服务。

		3) 采用国家密码管理局批准的双硬件物理噪声源生成真正随机数。 4) 支持密钥管理服务，采用“分层结构，逐层保护”的安全原则，提供管理密钥、用户密钥、会话密钥三层密钥体系，保证密钥的安全。 5) 设备内可存储 1024 对 SM2 密钥，密钥存储数量支持定制扩容。 6) 支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对。 7) 支持基于三五门限安全机制的密钥备份与恢复，且支持多版本备份恢复。 8) 支持分级权限管理，管理人员身份凭证信息安全存储在智能密码钥匙中；支持 CS/WEB 管理方式，并支持 SSL 协议确保通信的机密性。 9) 支持设备网口配置管理功能，可将网口设置为配置管理、主服务、兼容、聚合四种模式。 10) 支持日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **3、SSL VPN 综合安全网关：配置数量≥2 个** 1) 通过 SSL 安全网关，实现远程安全接入、访问权限控制、审计，用于云上信息系统与用户，云平台与云平台之间建立加密通道。提供 SSLVPNVPN 接入服务和 IPSECVPN 服务。 2) 支持国密算法套件，支持国密标准 SSL 协议 GMTLSv1.1，支持所有密码运算与密钥管理均通过硬件密码模块实现。 3) 支持 SSL 隧道端口复用配置，支持认证数据传输隧道和业务数据传输隧道隔离、合并两种数据传输要求 4) 支持 SSL 隧道保持机制可配置，包括不限于保活机制、超时机制。 5) 支持隧道传输保障技术，包括 IPSec 分片技术、MTU 探测修改技术，提高产品在复杂环境下的适应能力 6) 持抗非法报文攻击：包括 land 、Smurf、Ping of death、Winnuke、Tcp_sscan、Ip_option、Teardrop、Targa3、Ipspoof 等、支持通用非法报文、非法 TCP 报文、非法 ICMP 报文的检测、支持抗系统扫描，包括 Syn 半开扫描、FIN、ACK 扫描、圣诞树扫描、NULL 扫描、UDP 扫描等、支持抗洪泛攻击，包括 DOS、DDOS、SYNFLOOD、UDPFLOOD、PINGFLOOD 等 7) 支持虚子网，允许子网冲突。采用虚拟子网的方式，把原来冲突的网络转变为逻辑上重新规划的网络，冲突双方只需有一方配置了虚拟子网，就可以使得双方按照新的地址进行隧道访问，而原有访问 Internet 的地址和拓扑保持不变 8) 支持路由和透明工作模式，支持添加策略路由、静态路由，支持网桥功能，支持组播转发，支持链路均衡、链路备份。 9) 支持 NAT 穿越、支持双边 NAT 建隧道、支持 DPD 探测 10) 支持设置证书过滤规则，可通过对用户证书 C、ST、O、CN、L、OU、Email 等字段进行过滤，实现对接入用户的登入控制 11) 支持用户访问细粒度控制，支持用户组虚 IP 地址池，控制用户的访问时间、地址、资源等，支持同一个用户分配至多个用户组下，并支持组间隔离，支持用户黑名单 12) 支持多种短信认证服务，包含、串口短信设备、数据库短信设备、Web Service 短信设备、腾讯云短信 **4、时间戳服务器：** 1) 供时间戳签发、时间戳响应、时间戳解析时间戳和有效性等多种安全功能。

		2) 国密非对称密钥算法：SM2 算法。国密摘要算法：SM3 算法。国密对称秘钥算法：SM4 算法。 3) 支持符合 X509v3 标准格式的数字证书，提供第三方 CA 证书导入和管理功能，包括证书的导入管理、证书导出管 理和证书备份和恢复管理。 4) 证书支持多种文件格式的导入和使用，包括：cer、ebcer、pfx、p12、 p7b、zip 等。 5) 支持配置多信任 CA 签发的根证书，可验证不同 CA 机构签发的符合 PKCS#7 标准的签名、数字信封结果。 6) 支持多级信任链验证功能，支持业务白名单，只有在白名单中的业务系统才能访问服务器。 7) 支持管理员分权机制，包括但不限于超级管理员、管理员、审计员等。支持 Linux、AIX 等主流应用平台；支持 Java、COM、C 等应用集成接口；客户端支持国产操作系统，支持国产浏览器 。 8) 具有监控功能：分为业务监控和系统监控两种，并以图形化方式展示。业务监控包括打时间戳和验时间戳业务。系统监控包括 CPU、内存、硬盘和网络流量 9) 支持任务管理功能，能够查看审计日志导出任务，并显示当前全部任务 运行完成的百分比，用户可以对已完成的任务中的日志进行下载和删除任 务等管理操作。 10) 可以配置记录日志的类型譬如业务日志、管理员日志、Debug 日志、错误 日志，并可以根据需求开启或关闭。 11) 具有故障定位功能，针对错误打时间戳和验时间戳信息必须有详细的日志。 12) 支持一键巡检，液晶屏巡检功能，点击液晶屏按钮，显示巡检结果信息，对软件与硬件层面进行健康检查。 **5、身份认证网关** 1) 为业务系统提供基于基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务 2) 支持 TLS1.0、TLS1.1、TLS1.2、SSL3.0 协议；支持高安全性的 TLS1.3 协议；支持标准的国密 SSL 协议。 3) 支持多种认证方式：支持 UKEY 证书认证、协同签名、静态口令+验证码认证方式，支持基于数字证书的单、双向认证。 4) 支持证书+用户名口令联合登录：用户通过门户登录时，需要同时输入正确的用户名口令和选择正确的证书才可以登录成功。 5) 反向代理应用支持人脸二次认证：反向代理应用支持证书+人像认证，访问应用时进行证书认证后可以设定应用是否需要进行人像二次鉴别。 6) 支持 SSL 代理服务，可设置多个独立的 SSL/TLS 服务，通过服务端口进行不同区分，系统通过应用代理为应用发布单独的对外服务端口，用户通过身份认证网关的 IP 和对外服务端口访问应用。 7) 支持加密传输，客户端到网关之间的通信链路可以依据用户对安全和性能效率的需求选择是否加密，支持国密 SSL 加密传输。 8) 应用级访问控制：可根据用户认证方式、DN 规则、访问时间、源 IP、可信 CA、用户属性、角色、终端指纹等定制访问控制策略，符合规则条件的用户才有权限访问应用；支持 URL 级别的访问控制。 9) 支持证书认证后，可以把结果、用户的基本信息传送给后台的应用系统，应用系统实现单点；支持定义多种属性信息传递项：证书基本信息 DN 项、证书扩展信息、自定义扩展信息、用户属性信息、应用账号信息、客户端信息等属性，支持自定义属性信息。

		10）支持 CRL 列表自动更新失败后，该 CA 下的所有证书禁止登录功能。 11）支持反向穿透：支持主路部署模式下网关内保护的应用向网关外用户客户端发起连接的应用场景。 12）支持 portal 页面配置，可以配置公告信息、隐藏应用列表、自动打开应用列表、证书过期提示等信息。 13）支持液晶屏显示 CPU 利用率、IP 地址和版本信息。 **6、协同签名服务器** 1） 用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥生成、密钥签名、密钥解密、密钥协同功能。 2） 支持协同签名模块 App 集中发布，支持扫码安装，实现快速部署。 3） 支持 PC 版密码模块安装包的上传、下载、配置等管理功能。 4） 支持通过 PIN 码重置方式实现远程解锁功能，简化管理员日常管理、维护工作，支持自动审核 5） 配合移动终端密码模块、PC 端密码模块完成密钥分散、密钥存储、密钥运算等功能。 6） 配合移动终端完成数字证书全生命周期管理功能，如证书申请、更新、延期、注销等。 7） 支持移动终端证书更新策略、延期策略配置。 8） 支持安装包策略进行统一配置，简化实施、部署复杂度。 9） 支持系统备份功能，对系统重要数据、配置等进行备份。支持自动备份功能。 10）支持通过 web 方式对系统进行升级，方便日常运维、管理。 11）支持对系统重要服务进行启停管理。 **7、数据库透明加密系统** 1） 提供数据库资产智能梳理，精准识别和分类数据库中的各类资产。提供数据库指令的访问控制，对数据库访问指令进行严格审查，确保只有合法的指令才能执行，防止恶意操作。提供数据库透明加解密能力，对数据库中的核敏字段进行加密存储，采用高强度加密算法，保障敏感数据在存储过程中的安全性。在数据展示和传输过程中，通过数据内容动态脱敏技术，自动对敏感信息进行脱敏处理，降低数据泄露风险，全方位守护用户数据安全，有效防止未授权访问和数据泄露事件的发生。 2） 支持对数据库的库表识别能力，可根据手动配置的数据库、数据库表、数据库表字段等信息用于数据分析识别。在数据库识别过程中，主动模式和被动模式，主动模式根据数据库安全网关将通过账号密码主动连接数据库，被动模式是用户通过数据库网关访问数据库时，被动完成数据库发现动作。 3） 支持对数据库地址、授权状态、版本、数据库名称、服务器地址、防护状态的启停、连接状态的信息回显等。支持数据库网关在管理过程中对受保护的数据库启用保护状态功能，可查看数据库连接状态；支持对受保护的数据库进行数据立即同步动作；支持添加数据库管理维护数据库使用的账号，用于在数据权限管理处基于数据库账号进行细粒度授权。 4） 支持对内置的分类分级标准库中的数据分类进行手动编辑，可按照行业最新的数据重要级别进行自定义分类，编辑类型包含编码、分类名称。可删除当前分类，添加分类或子分类中包含分类编码、分类名称、脱敏算法、安全等级等。 5） 支持基于数据库账户和应用账户，对数据库“增、删、改、查”指令进行指令级管控，实现数据库的指令级访问控制。 6） 支持基于数据库账户和应用账户，对数据库表中的敏感字段在存

		储和读取阶段进行数据动态加解密，实现关键数据字段拖库等方式的防泄露。 7） 支持基于数据库账户和应用账户，对数据库表中的敏感字段进行数据动态脱敏，实现数据库关键数据使用和展示阶段的数据防泄漏。 8） 支持全局敏感数据自动标注管理，对标注规则可编辑，编辑内容包含规则名称、规则状态、标注内容、分类、分级、脱敏算法等。 9） 内置脱敏算法中包含国内手机号、电子邮件地址、通用身份证号、电话号码、银行卡函、中国身份证号码、年龄、IPV4、IPV6、姓名、车牌号等 30 多种类型。支持添加自定义算法，自定义内容包含算法名称、算法描述、脱敏类型（部分替换、完全替换、指定算法处理）、测试等。 10） 管理员可自定义数据加密方式，如 SM4 等，并支持秘钥更新周管理。新增加密套件支持本地加密和远程加密方式，且秘钥支持备份功能，支持本地本地和远程备份功能。 11） 支持对数据库访问行为进行记录，记录的日志包括用户、源 IP、归属地、终端名称、数据库、数据表、请求类型、执行动作、次数等。 **8、文档加密网关** 1） 提供非结构化文件加密服务，采用安全合规且先进的加密算法，确保文件在存储和传输过程中数据的机密性。对非结构化业务服务器接口实施严格的访问控制，通过精细化的权限管理，防止未授权、越权访问和渗透攻击，保障接口的安全性。提供业务服务器 Web 数据动态脱敏功能，在数据展示和传输过程中，能够自动对敏感信息进行脱敏处理，降低数据泄露风险，从而全方位保障用户数据的安全性、可见性和合规性。 2） 支持 B/S 业务系统的文件上传加密，在文件存储服务器上以密文格式存储相关文件。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 3） 支持 B/S 业务系统的文件下载加密，将文件服务器上的加密文件解密还原后，发送到授权终端，供授权终端正常使用。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 4） 支持文件传输过程中的断点续传，保障大文件的传输稳定性。 5） 支持国密的加解密算法。 6） 支持自动备份密钥套件至加密文件，支持 FTP、SCP 协议的备份。 7） 支持通过指定加密密钥文件的完全离线解密数据能力，支持历史数据通过离线加解密工具进行离线解密。 8） 支持 B/S 业务系统开启接口自动发现功能，自动获取并梳理业务系统的所有接口以及接口下的各个数据字段。 9） 支持对业务系统的接口字段进行数据脱敏，数据脱敏默认以全“*”脱敏，针对需要特殊处理的脱敏字段，支持自定义的数据脱敏规则和算法。 10） 支持对 SQL 注入攻击、XSS 攻击、CC 攻击、远程命令攻击等常见 web 攻击行为进行防御。 11） 支持文件加解密日志、攻击事件日志和业务资产安全访问日志。
5	云密码资源池硬件	**9、云服务器密码机：配置数量≥2 台** 10） 采用了密钥管理与设备管理分离的核心理念，实现了云应用环境下网络管理员仅维护设备，用户自行管理密钥的工作模式。云密码机通过密码机集群与虚拟化技术的结合扩充密码运算能力，将

		密码运算能力进行细粒度划分，并通过集中的密钥管理及配套的安全策略保护用户密钥整生命周期的安全。 11）云服务器密码机支持基于 KVM 的虚拟化技术，在一个 CHSM 中虚拟出多个 VSM，内置支持 SR-IOV 虚拟化技术的硬件密码卡，提供密码模块的虚拟化支撑能力。 12）云服务器密码机支持采用安全隔离技术，对每个 VSM 使用的密钥在存储和使用上进行了安全隔离。 13）★云服务器密码机支持创建不同规格与性能的虚拟密码机；云服务器密码机支持利用负载均衡技术实现虚拟化实例对密码资源占用的分配，管理系统可以根据实际情况动态增加或释放密码运算资源。 14）云服务器密码机支持 VLAN 池划分，当虚拟机选择同一个 VLAN 后，只同一个 VLAN 内的虚拟机可以互相访问，与其他虚拟机无法通信。 15）云服务器密码机支持国密 SSH、国密 FTP，保证整机运维安全。 16）云服务器密码机管理接口符合《云服务器密码机管理接口规范》的要求，可提供 CHSM 及 VSM 的配置管理接口。 17）云服务器密码机支持多种国密算法，主要包括 SM1、SM2、SM3、SM4、等国密算法。 18）★云服务器密码机支持虚拟机日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **10、服务器密码机：配置数量≥2 台** 11）支持 SM1、SM2、SM3、SM4 国密算法。 12）可提供对称算法加解密、非对称算法加密、解密、签名、验证，消息鉴别码产生与验证等密码服务。 13）采用国家密码管理局批准的双硬件物理噪声源生成真正随机数，随机数质量高。 14）支持密钥管理服务，采用“分层结构，逐层保护”的安全原则，提供管理密钥、用户密钥、会话密钥三层密钥体系，保证密钥的安全。 15）设备内可存储 1024 对 SM2 密钥，密钥存储数量支持定制扩容。 16）支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对。 17）支持基于三五门限安全机制的密钥备份与恢复，且支持多版本备份恢复。 18）支持分级权限管理，管理人员身份凭证信息安全存储在智能密码钥匙中；支持 CS/WEB 管理方式，并支持 SSL 协议确保通信的机密性。 19）支持设备网口配置管理功能，可将网口设置为配置管理、主服务、兼容、聚合四种模式。 20）支持日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **11、SSL VPN 综合安全网关：配置数量≥2 个** 13）通过 SSL 安全网关，实现远程安全接入、访问权限控制、审计，用于云上信息系统与用户，云平台与云平台之间建立加密通道。提供 SSLVPNVPN 接入服务和 IPSECVPN 服务。 14）支持国密算法套件，支持国密标准 SSL 协议 GMTLSv1.1，支持所有密码运算与密钥管理均通过硬件密码模块实现。 15）支持 SSL 隧道端口复用配置，支持认证数据传输隧道和业务数据传输隧道隔离、合并两种数据传输要求

		16) 支持 SSL 隧道保持机制可配置，包括不限于保活机制、超时机制。 17) 支持隧道传输保障技术，包括 IPSec 分片技术、MTU 探测修改技术，提高产品在复杂环境下的适应能力 18) 持抗非法报文攻击：包括 land 、Smurf、Ping of death、Winnuke、Tcp_sscan、Ip_option、Teardrop、Targa3、Ipspoof 等、支持通用非法报文、非法 TCP 报文、非法 ICMP 报文的检测、支持抗系统扫描，包括 Syn 半开扫描、FIN、ACK 扫描、圣诞树扫描、NULL 扫描、UDP 扫描等、支持抗洪泛攻击，包括 DOS、DDOS、SYNFLOOD、UDPFLOOD、PINGFLOOD 等 19) 支持虚子网，允许子网冲突。采用虚拟子网的方式，把原来冲突的网络转变为逻辑上重新规划的网络，冲突双方只需有一方配置了虚拟子网，就可以使得双方按照新的地址进行隧道访问，而原有访问 Internet 的地址和拓扑保持不变 20) 支持路由和透明工作模式，支持添加策略路由、静态路由，支持网桥功能，支持组播转发，支持链路均衡、链路备份。 21) 支持 NAT 穿越、支持双边 NAT 建隧道、支持 DPD 探测 22) 支持设置证书过滤规则，可通过对用户证书 C、ST、O、CN、L、OU、Email 等字段进行过滤，实现对接入用户的登入控制 23) 支持用户访问细粒度控制，支持用户组虚 IP 地址池，控制用户的访问时间、地址、资源等，支持同一个用户分配至多个用户组下，并支持组间隔离，支持用户黑名单 24) 支持多种短信认证服务，包含、串口短信设备、数据库短信设备、Web Service 短信设备 **12、时间戳服务器：** 13) 供时间戳签发、时间戳响应、时间戳解析时间戳和有效性等多种安全功能。 14) 国密非对称密钥算法：SM2 算法。国密摘要算法：SM3 算法。国密对称秘钥算法：SM4 算法。 15) 支持符合 X509v3 标准格式的数字证书，提供第三方 CA 证书导入和管理功能，包括证书的导入管理、证书导出管 理和证书备份和恢复管理。 16) 证书支持多种文件格式的导入和使用，包括：cer、ebcer、pfx、p12、 p7b、zip 等。 17) 支持配置多信任 CA 签发的根证书，可验证不同 CA 机构签发的符合 PKCS#7 标准的签名、数字信封结果。 18) 支持多级信任链验证功能，支持业务白名单，只有在白名单中的业务系统才能访问服务器。 19) 支持管理员分权机制，包括但不限于超级管理员、管理员、审计员等。支持 Linux、AIX 等主流应用平台；支持 Java、COM、C 等应用集成接口；客户端支持国产操作系统，支持国产浏览器 。 20) 具有监控功能：分为业务监控和系统监控两种，并以图形化方式展示。业务监控包括打时间戳和验时间戳业务。系统监控包括 CPU、内存、硬盘和网络流量 21) 支持任务管理功能，能够查看审计日志导出任务，并显示当前全部任务 运行完成的百分比，用户可以对已完成的任务中的日志进行下载和删除任 务等管理操作。 22) 可以配置记录日志的类型譬如业务日志、管理员日志、Debug 日志、错误 日志，并可以根据需求开启或关闭。 23) 具有故障定位功能，针对错误打时间戳和验时间戳信息必须有详细的日志。 24) 支持一键巡检，液晶屏巡检功能，点击液晶屏按钮，显示巡检结

		果信息，对软件与硬件层面进行健康检查。 **13、身份认证网关** 14) 为业务系统提供基于基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务 15) 支持 TLS1.0、TLS1.1、TLS1.2、SSL3.0 协议；支持高安全性的 TLS1.3 协议；支持标准的国密 SSL 协议。 16) 支持多种认证方式：支持 UKEY 证书认证、协同签名、静态口令+验证码认证方式，支持基于数字证书的单、双向认证。 17) 支持证书+用户名口令联合登录：用户通过门户登录时，需要同时输入正确的用户名口令和选择正确的证书才可以登录成功。 18) 反向代理应用支持人脸二次认证：反向代理应用支持证书+人像认证，访问应用时进行证书认证后可以设定应用是否需要进行人像二次鉴别。 19) 支持 SSL 代理服务，可设置多个独立的 SSL/TLS 服务，通过服务端口进行不同区分，系统通过应用代理为应用发布单独的对外服务端口，用户通过身份认证网关的 IP 和对外服务端口访问应用。 20) 支持加密传输，客户端到网关之间的通信链路可以依据用户对安全和性能效率的需求选择是否加密，支持国密 SSL 加密传输。 21) 应用级访问控制：可根据用户认证方式、DN 规则、访问时间、源 IP、可信 CA、用户属性、角色、终端指纹等定制访问控制策略，符合规则条件的用户才有权限访问应用；支持 URL 级别的访问控制。 22) 支持证书认证后，可以把结果、用户的基本信息传送给后台的应用系统，应用系统实现单点；支持定义多种属性信息传递项：证书基本信息 DN 项、证书扩展信息、自定义扩展信息、用户属性信息、应用账号信息、客户端信息等属性，支持自定义属性信息。 23) 支持 CRL 列表自动更新失败后,该 CA 下的所有证书禁止登录功能。 24) 支持反向穿透：支持主路部署模式下网关内保护的应用向网关外用户客户端发起连接的应用场景。 25) 支持 portal 页面配置，可以配置公告信息、隐藏应用列表、自动打开应用列表、证书过期提示等信息。 26) 支持液晶屏显示 CPU 利用率、IP 地址和版本信息。 **14、协同签名服务器** 12) 用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥生成、密钥签名、密钥解密、密钥协同功能。 13) 支持协同签名模块 App 集中发布，支持扫码安装，实现快速部署。 14) 支持 PC 版密码模块安装包的上传、下载、配置等管理功能。 15) 支持通过 PIN 码重置方式实现远程解锁功能，简化管理员日常管理、维护工作，支持自动审核 16) 配合移动终端密码模块、PC 端密码模块完成密钥分散、密钥存储、密钥运算等功能。 17) 配合移动终端完成数字证书全生命周期管理功能，如证书申请、更新、延期、注销等。 18) 支持移动终端证书更新策略、延期策略配置。 19) 支持安装包策略进行统一配置，简化实施、部署复杂度。 20) 支持系统备份功能，对系统重要数据、配置等进行备份。支持自动备份功能。 21) 支持通过 web 方式对系统进行升级，方便日常运维、管理。 22) 支持对系统重要服务进行启停管理。 **15、数据库透明加密系统**

		12) 提供数据库资产智能梳理，精准识别和分类数据库中的各类资产。提供数据库指令的访问控制，对数据库访问指令进行严格审查，确保只有合法的指令才能执行，防止恶意操作。提供数据库透明加解密能力，对数据库中的核敏字段进行加密存储，采用高强度加密算法，保障敏感数据在存储过程中的安全性。在数据展示和传输过程中，通过数据内容动态脱敏技术，自动对敏感信息进行脱敏处理，降低数据泄露风险，全方位守护用户数据安全，有效防止未授权访问和数据泄露事件的发生。 13) 支持对数据库的库表识别能力，可根据手动配置的数据库、数据库表、数据库表字段等信息用于数据分析识别。在数据库识别过程中，主动模式和被动模式，主动模式根据数据库安全网关将通过账号密码主动连接数据库，被动模式是用户通过数据库网关访问数据库时，被动完成数据库发现动作。 14) 支持对数据库地址、授权状态、版本、数据库名称、服务器地址、防护状态的启停、连接状态的信息回显等。支持数据库网关在管理过程中对受保护的数据库启用保护状态功能，可查看数据库连接状态；支持对受保护的数据库进行数据立即同步动作；支持添加数据库管理维护数据库使用的账号，用于在数据权限管理处基于数据库账号进行细粒度授权。 15) 支持对内置的分类分级标准库中的数据分类进行手动编辑，可按照行业最新的数据重要级别进行自定义分类，编辑类型包含编码、分类名称。可删除当前分类，添加分类或子分类中包含分类编码、分类名称、脱敏算法、安全等级等。 16) 支持基于数据库账户和应用账户，对数据库“增、删、改、查”指令进行指令级管控，实现数据库的指令级访问控制。 17) 支持基于数据库账户和应用账户，对数据库表中的敏感字段在存储和读取阶段进行数据动态加解密，实现关键数据字段拖库等方式的防泄露。 18) 支持基于数据库账户和应用账户，对数据库表中的敏感字段进行数据动态脱敏，实现数据库关键数据使用和展示阶段的数据防泄漏。 19) 支持全局敏感数据自动标注管理，对标注规则可编辑，编辑内容包含规则名称、规则状态、标注内容、分类、分级、脱敏算法等。 20) 内置脱敏算法中包含国内手机号、电子邮件地址、通用身份证号、电话号码、银行卡函、中国身份证号码、年龄、IPV4、IPV6、姓名、车牌号等 30 多种类型。支持添加自定义算法，自定义内容包含算法名称、算法描述、脱敏类型（部分替换、完全替换、指定算法处理）、测试等。 21) 管理员可自定义数据加密方式，如 SM4 等，并支持秘钥更新周管理。新增加密套件支持本地加密和远程加密方式，且秘钥支持备份功能，支持本地本地和远程备份功能。 22) 支持对数据库访问行为进行记录，记录的日志包括用户、源 IP、归属地、终端名称、数据库、数据表、请求类型、执行动作、次数等。 **16、文档加密网关** 12) 提供非结构化文件加密服务，采用安全合规且先进的加密算法，确保文件在存储和传输过程中数据的机密性。对非结构化业务服务器接口实施严格的访问控制，通过精细化的权限管理，防止未授权、越权访问和渗透攻击，保障接口的安全性。提供业务服务器 Web 数据动态脱敏功能，在数据展示和传输过程中，能够自动对敏感信息进行脱敏处理，降低数据泄露风险，从而全方位保障

		用户数据的安全性、可见性和合规性。 13) 支持 B/S 业务系统的文件上传加密，在文件存储服务器上以密文格式存储相关文件。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 14) 支持 B/S 业务系统的文件下载加密，将文件服务器上的加密文件解密还原后，发送到授权终端，供授权终端正常使用。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 15) 支持文件传输过程中的断点续传，保障大文件的传输稳定性。 16) 支持国密的加解密算法。 17) 支持自动备份密钥套件至加密文件，支持 FTP、SCP 协议的备份。 18) 支持通过指定加密密钥文件的完全离线解密数据能力，支持历史数据通过离线加解密工具进行离线解密。 19) 支持 B/S 业务系统开启接口自动发现功能，自动获取并梳理业务系统的所有接口以及接口下的各个数据字段。 20) 支持对业务系统的接口字段进行数据脱敏，数据脱敏默认以全“*”脱敏，针对需要特殊处理的脱敏字段，支持自定义的数据脱敏规则和算法。 21) 支持对 SQL 注入攻击、XSS 攻击、CC 攻击、远程命令攻击等常见 web 攻击行为进行防御。 22) 支持文件加解密日志、攻击事件日志和业务资产安全访问日志。
6	云密码资源池硬件	**17、云服务器密码机：配置数量≥2 台** 19) 采用了密钥管理与设备管理分离的核心理念，实现了云应用环境下网络管理员仅维护设备，用户自行管理密钥的工作模式。云密码机通过密码机集群与虚拟化技术的结合扩充密码运算能力，将密码运算能力进行细粒度划分，并通过集中的密钥管理及配套的安全策略保护用户密钥整生命周期的安全。 20) 云服务器密码机支持基于 KVM 的虚拟化技术，在一个 CHSM 中虚拟出多个 VSM，内置支持 SR-IOV 虚拟化技术的硬件密码卡，提供密码模块的虚拟化支撑能力。 21) 云服务器密码机支持采用安全隔离技术，对每个 VSM 使用的密钥在存储和使用上进行了安全隔离。 22) ★云服务器密码机支持创建不同规格与性能的虚拟密码机；云服务器密码机支持利用负载均衡技术实现虚拟化实例对密码资源占用的分配，管理系统可以根据实际情况动态增加或释放密码运算资源。 23) 云服务器密码机支持 VLAN 池划分，当虚拟机选择同一个 VLAN 后，只同一个 VLAN 内的虚拟机可以互相访问，与其他虚拟机无法通信。 24) 云服务器密码机支持国密 SSH、国密 FTP，保证整机运维安全。 25) 云服务器密码机管理接口符合《云服务器密码机管理接口规范》的要求，可提供 CHSM 及 VSM 的配置管理接口。 26) 云服务器密码机支持多种国密算法，主要包括 SM1、SM2、SM3、SM4、等国密算法。 27) ★云服务器密码机支持虚拟机日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **18、服务器密码机：配置数量≥2 台** 21) 支持 SM1、SM2、SM3、SM4 国密算法。 22) 可提供对称算法加解密、非对称算法加密、解密、签名、验证，消息鉴别码产生与验证等密码服务。

		23）采用国家密码管理局批准的双硬件物理噪声源生成真正随机数，随机数质量高。 24）支持密钥管理服务，采用“分层结构，逐层保护”的安全原则，提供管理密钥、用户密钥、会话密钥三层密钥体系，保证密钥的安全。 25）设备内可存储 1024 对 SM2 密钥，密钥存储数量支持定制扩容。 26）支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对。 27）支持基于三五门限安全机制的密钥备份与恢复，且支持多版本备份恢复。 28）支持分级权限管理，管理人员身份凭证信息安全存储在智能密码钥匙中；支持 CS/WEB 管理方式，并支持 SSL 协议确保通信的机密性。 29）支持设备网口配置管理功能，可将网口设置为配置管理、主服务、兼容、聚合四种模式。 30）支持日志等级设置，可设置为 DEBUG、WARN、ERROR、FATAL 四个等级，且支持通过数字签名的方式实现日志数据完整性保护。 **19、SSL VPN 综合安全网关：配置数量≥2 个** 25）通过 SSL 安全网关，实现远程安全接入、访问权限控制、审计，用于云上信息系统与用户，云平台与云平台之间建立加密通道。提供 SSLVPNVPN 接入服务和 IPSECVPN 服务。 26）支持国密算法套件，支持国密标准 SSL 协议 GMTLSv1.1，支持所有密码运算与密钥管理均通过硬件密码模块实现。 27）支持 SSL 隧道端口复用配置，支持认证数据传输隧道和业务数据传输隧道隔离、合并两种数据传输要求 28）支持 SSL 隧道保持机制可配置，包括不限于保活机制、超时机制。 29）支持隧道传输保障技术，包括 IPSec 分片技术、MTU 探测修改技术，提高产品在复杂环境下的适应能力 30）持抗非法报文攻击：包括 land 、Smurf、Ping of death、Winnuke、Tcp_sscan、Ip_option、Teardrop、Targa3、Ipspoof 等、支持通用非法报文、非法 TCP 报文、非法 ICMP 报文的检测、支持抗系统扫描，包括 Syn 半开扫描、FIN、ACK 扫描、圣诞树扫描、NULL 扫描、UDP 扫描等、支持抗洪泛攻击，包括 DOS、DDOS、SYNFLOOD、UDPFLOOD、PINGFLOOD 等 31）支持虚子网，允许子网冲突。采用虚拟子网的方式，把原来冲突的网络转变为逻辑上重新规划的网络，冲突双方只需有一方配置了虚拟子网，就可以使得双方按照新的地址进行隧道访问，而原有访问 Internet 的地址和拓扑保持不变 32）支持路由和透明工作模式，支持添加策略路由、静态路由，支持网桥功能，支持组播转发，支持链路均衡、链路备份。 33）支持 NAT 穿越、支持双边 NAT 建隧道、支持 DPD 探测 34）支持设置证书过滤规则，可通过对用户证书 C、ST、O、CN、L、OU、Email 等字段进行过滤，实现对接入用户的登入控制 35）支持用户访问细粒度控制，支持用户组虚 IP 地址池，控制用户的访问时间、地址、资源等，支持同一个用户分配至多个用户组下，并支持组间隔离，支持用户黑名单 36）支持多种短信认证服务，包含、串口短信设备、数据库短信设备、Web Service 短信设备、腾讯云短信 **20、时间戳服务器：** 25）供时间戳签发、时间戳响应、时间戳解析时间戳和有效性等多种

		安全功能。 26) 国密非对称密钥算法：SM2 算法。国密摘要算法：SM3 算法。国密对称秘钥算法：SM4 算法。 27) 支持符合 X509v3 标准格式的数字证书，提供第三方 CA 证书导入和管理功能，包括证书的导入管理、证书导出管 理和证书备份和恢复管理。 28) 证书支持多种文件格式的导入和使用，包括：cer、ebcer、pfx、p12、 p7b、zip 等。 29) 支持配置多信任 CA 签发的根证书，可验证不同 CA 机构签发的符合 PKCS#7 标准的签名、数字信封结果。 30) 支持多级信任链验证功能，支持业务白名单，只有在白名单中的业务系统才能访问服务器。 31) 支持管理员分权机制，包括但不限于超级管理员、管理员、审计员等。支持 Linux、AIX 等主流应用平台；支持 Java、COM、C 等应用集成接口；客户端支持国产操作系统，支持国产浏览器 。 32) 具有监控功能：分为业务监控和系统监控两种，并以图形化方式展示。业务监控包括打时间戳和验时间戳业务。系统监控包括 CPU、内存、硬盘和网络流量 33) 支持任务管理功能，能够查看审计日志导出任务，并显示当前全部任务 运行完成的百分比，用户可以对已完成的任务中的日志进行下载和删除任 务等管理操作。 34) 可以配置记录日志的类型譬如业务日志、管理员日志、Debug 日志、错误 日志，并可以根据需求开启或关闭。 35) 具有故障定位功能，针对错误打时间戳和验时间戳信息必须有详细的日志。 36) 支持一键巡检，液晶屏巡检功能，点击液晶屏按钮，显示巡检结果信息，对软件与硬件层面进行健康检查。 **21、身份认证网关** 27) 为业务系统提供基于基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务 28) 支持 TLS1.0、TLS1.1、TLS1.2、SSL3.0 协议；支持高安全性的 TLS1.3 协议；支持标准的国密 SSL 协议。 29) 支持多种认证方式：支持 UKEY 证书认证、协同签名、静态口令+验证码认证方式，支持基于数字证书的单、双向认证。 30) 支持证书+用户名口令联合登录：用户通过门户登录时，需要同时输入正确的用户名口令和选择正确的证书才可以登录成功。 31) 反向代理应用支持人脸二次认证：反向代理应用支持证书+人像认证，访问应用时进行证书认证后可以设定应用是否需要进行人像二次鉴别。 32) 支持 SSL 代理服务，可设置多个独立的 SSL/TLS 服务，通过服务端口进行不同区分，系统通过应用代理为应用发布单独的对外服务端口，用户通过身份认证网关的 IP 和对外服务端口访问应用。 33) 支持加密传输，客户端到网关之间的通信链路可以依据用户对安全和性能效率的需求选择是否加密，支持国密 SSL 加密传输。 34) 应用级访问控制：可根据用户认证方式、DN 规则、访问时间、源 IP、可信 CA、用户属性、角色、终端指纹等定制访问控制策略，符合规则条件的用户才有权限访问应用；支持 URL 级别的访问控制。 35) 支持证书认证后，可以把结果、用户的基本信息传送给后台的应用系统，应用系统实现单点；支持定义多种属性信息传递项：证书基本信息 DN 项、证书扩展信息、自定义扩展信息、用户属性信

		息、应用账号信息、客户端信息等属性，支持自定义属性信息。 36) 支持 CRL 列表自动更新失败后,该 CA 下的所有证书禁止登录功能。 37) 支持反向穿透：支持主路部署模式下网关内保护的应用向网关外用户客户端发起连接的应用场景。 38) 支持 portal 页面配置，可以配置公告信息、隐藏应用列表、自动打开应用列表、证书过期提示等信息。 39) 支持液晶屏显示 CPU 利用率、IP 地址和版本信息。 **22、协同签名服务器** 23) 用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥生成、密钥签名、密钥解密、密钥协同功能。 24) 支持协同签名模块 App 集中发布，支持扫码安装，实现快速部署。 25) 支持 PC 版密码模块安装包的上传、下载、配置等管理功能。 26) 支持通过 PIN 码重置方式实现远程解锁功能，简化管理员日常管理、维护工作，支持自动审核 27) 配合移动终端密码模块、PC 端密码模块完成密钥分散、密钥存储、密钥运算等功能。 28) 配合移动终端完成数字证书全生命周期管理功能，如证书申请、更新、延期、注销等。 29) 支持移动终端证书更新策略、延期策略配置。 30) 支持安装包策略进行统一配置，简化实施、部署复杂度。 31) 支持系统备份功能，对系统重要数据、配置等进行备份。支持自动备份功能。 32) 支持通过 web 方式对系统进行升级，方便日常运维、管理。 33) 支持对系统重要服务进行启停管理。 **23、数据库透明加密系统** 23) 提供数据库资产智能梳理，精准识别和分类数据库中的各类资产。提供数据库指令的访问控制，对数据库访问指令进行严格审查，确保只有合法的指令才能执行，防止恶意操作。提供数据库透明加解密能力，对数据库中的核敏字段进行加密存储，采用高强度加密算法，保障敏感数据在存储过程中的安全性。在数据展示和传输过程中，通过数据内容动态脱敏技术，自动对敏感信息进行脱敏处理，降低数据泄露风险，全方位守护用户数据安全，有效防止未授权访问和数据泄露事件的发生。 24) 支持对数据库的库表识别能力，可根据手动配置的数据库、数据库表、数据库表字段等信息用于数据分析识别。在数据库识别过程中，主动模式和被动模式，主动模式根据数据库安全网关将通过账号密码主动连接数据库，被动模式是用户通过数据库网关访问数据库时，被动完成数据库发现动作。 25) 支持对数据库地址、授权状态、版本、数据库名称、服务器地址、防护状态的启停、连接状态的信息回显等。支持数据库网关在管理过程中对受保护的数据库启用保护状态功能，可查看数据库连接状态；支持对受保护的数据库进行数据立即同步动作；支持添加数据库管理维护数据库使用的账号，用于在数据权限管理处基于数据库账号进行细粒度授权。 26) 支持对内置的分类分级标准库中的数据分类进行手动编辑，可按照行业最新的数据重要级别进行自定义分类，编辑类型包含编码、分类名称。可删除当前分类，添加分类或子分类中包含分类编码、分类名称、脱敏算法、安全等级等。 27) 支持基于数据库账户和应用账户，对数据库“增、删、改、查”指令进行指令级管控，实现数据库的指令级访问控制。

		28）支持基于数据库账户和应用账户，对数据库表中的敏感字段在存储和读取阶段进行数据动态加解密，实现关键数据字段拖库等方式的防泄露。 29）支持基于数据库账户和应用账户，对数据库表中的敏感字段进行数据动态脱敏，实现数据库关键数据使用和展示阶段的数据防泄漏。 30）支持全局敏感数据自动标注管理，对标注规则可编辑，编辑内容包含规则名称、规则状态、标注内容、分类、分级、脱敏算法等。 31）内置脱敏算法中包含国内手机号、电子邮件地址、通用身份证号、电话号码、银行卡函、中国身份证号码、年龄、IPV4、IPV6、姓名、车牌号等 30 多种类型。支持添加自定义算法，自定义内容包含算法名称、算法描述、脱敏类型（部分替换、完全替换、指定算法处理）、测试等。 32）管理员可自定义数据加密方式，如 SM4 等，并支持秘钥更新周管理。新增加密套件支持本地加密和远程加密方式，且秘钥支持备份功能，支持本地本地和远程备份功能。 33）支持对数据库访问行为进行记录，记录的日志包括用户、源 IP、归属地、终端名称、数据库、数据表、请求类型、执行动作、次数等。 **24、文档加密网关** 23）提供非结构化文件加密服务，采用安全合规且先进的加密算法，确保文件在存储和传输过程中数据的机密性。对非结构化业务服务器接口实施严格的访问控制，通过精细化的权限管理，防止未授权、越权访问和渗透攻击，保障接口的安全性。提供业务服务器 Web 数据动态脱敏功能，在数据展示和传输过程中，能够自动对敏感信息进行脱敏处理，降低数据泄露风险，从而全方位保障用户数据的安全性、可见性和合规性。 24）支持 B/S 业务系统的文件上传加密，在文件存储服务器上以密文格式存储相关文件。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 25）支持 B/S 业务系统的文件下载加密，将文件服务器上的加密文件解密还原后，发送到授权终端，供授权终端正常使用。支持业务系统使用过程中的透明加解密，无需安装客户端加解密工具、无需集成 SDK 或加密接口调用，业务系统无改造。 26）支持文件传输过程中的断点续传，保障大文件的传输稳定性。 27）支持国密的加解密算法。 28）支持自动备份密钥套件至加密文件，支持 FTP、SCP 协议的备份。 29）支持通过指定加密密钥文件的完全离线解密数据能力，支持历史数据通过离线加解密工具进行离线解密。 30）支持 B/S 业务系统开启接口自动发现功能，自动获取并梳理业务系统的所有接口以及接口下的各个数据字段。 31）支持对业务系统的接口字段进行数据脱敏，数据脱敏默认以全“*”脱敏，针对需要特殊处理的脱敏字段，支持自定义的数据脱敏规则和算法。 32）支持对 SQL 注入攻击、XSS 攻击、CC 攻击、远程命令攻击等常见 web 攻击行为进行防御。 33）支持文件加解密日志、攻击事件日志和业务资产安全访问日志。
7	驻场运维服务	1、负责政务云安全资源池、云密码资源池日常运维检查。主要包括：产品状态检查、日志等。 2、源池的稳定运行，并提供日报和周报。

		3、负责资源池自动化配置核查与分析、提供专业的合规性报表和安全配置项建议，并进行配置优化。出具安全配置建议书，并定期根据实时互联网威胁和重大漏洞更新。 4、负责资源池的系统状态监控，日志分析、安全事件分析分类处理的工作；同时可根据发生事件的严重程度进行事件判别、通报、配合启动应急预案，提交应急预案文档。 5、负责每季度对资源池进行安全脆弱性和高危漏洞检测，并提供详细的解决方案，对资源池进行全面的安全风险审计，并提供详细的安全审计报告。 6、在国庆、两会以及护网行动演习等重保时期提供安全检查、安全监控等重保服务，出现网络安全事件时提供应急响应，协助处理安全事件，提供 7*24 小时现场值守服务。 7、渗透测试服务。根据用户要求，定期提供渗透测试服务，提供渗透测试报告和安全整改及加固建议。 8、每月按时提供各个租户的安全运维报告和政务云安全运营报告。

售后服务内容及要求：

2.1 质量保证：按本项目的行业规则或双方签订合同时的约定执行。质保期内如果出现质量问题，成交供应商应当无条件更换，由于质量问题造成的损失由成交供应商负全部责任。

2.2 售后服务：在接到采购方服务请求后，1 小时响应，12 小时内上门解决问题；质保期内提供免费上门服务，质保期外的收费按相关行业规则或由双方协商收取。

2.3 服务地点：采购人指定地点。

2.4 服务期限：3 年。

2.5 质量标准：符合相关要求，合格。

2.6 验收：采取自行验收、组织专家验收、第三方验收等方式。

付款方式：

本项目采用运营服务模式，投标人依据采购人要求，投资建设政务云安全资源池、云密码资源池并负责系统运维。采购人向投标人结算以收到最终客户的结算款为基数，

结算金额=最终客户结算款*折扣率。

第四章 评标办法

一．总　则

第一条为了做好**本项目（项目编号：周财招标采购-2025-10 号）**的招标评标工作，保证项目评审工作的正常有序进行，维护采购人、投标人的合法权益，依据《中华人民共和国政府采购法》及其它相关法律法规，本着公开、公平、公正的原则，制定评标办法。

第二条 本次项目评标采用**综合评分法**作为对投标人标书的比较方法。

第三条 按照《中华人民共和国政府采购法》及其相关规定组成评标委员会负责本项目的评审工作。评标委员会在政府采购专家库中随机抽取。

第四条 评委会按照“客观公正，实事求是”的原则，评价参加本次招标的投标人所提供的产品价格、性能、质量、服务及对招标文件的符合性及响应性。

二．评标程序及评审细则

第五条 评标工作于开标后进行。评委会应认真研究招标文件，至少应了解和熟悉以下内容：

（一）招标的目标；

（二）招标项目的范围和性质；

（三）招标文件中规定的主要技术要求、标准和商务条款；

（四）招标文件规定的评标标准、评标方法和在评标过程中考虑的相关因素。

第六条 有效投标应符合以下原则：

（一）满足招标文件的实质性要求；

（二）无重大偏离、保留或采购人不能接受的附加条件；

（三）通过投标符合性审查；

（四）评委会依据招标文件认定的其他原则；

（五）商务偏差表或技术偏差表数据不存在弄虚作假现象；

（六）投标人报价未超过采购人的采购预算；

第七条 评委会从每个投标人的投标文件开始独立评审，对开标后投标人所提出的优惠条件不予以考虑。按综合得分从高到低的顺序评出中标候选人。

第八条 评审中，评委会发现投标人的投标文件中对同类问题表述不一致、前后矛盾、有明显文字和计算错误的内容、有可能不符合招标文件规定等情况需要澄清时，评委会将以询标的方式告知并要求投标人以书面方式进行必要的澄清、说明或补正。对于询标后判

定为不符合招标文件的投标文件，评委要提出充足的否定理由。

第九条 评委会首先对各投标人进行符合性审查，通过符合性审查的投标人为有效投标人，有效投标人进入综合评分环节，按招标文件约定由评委会推荐中标候选人；没有通过符合性审查的投标人为无效投标。

项目符合性审查表				
序号	指标名称	指标要求	是否通过	投标文件格式及提交资料要求
1	投标人资格	见招标文件		见投标文件
2	技术要求	按评标办法		见投标文件
3	质保及售后等	见招标文件		见投标文件

评分标准（满分为 100 分）说明:各投标人的最终得分为各评委得分的算术平均值；评分分值计算保留小数点后两位，小数点后第三位“四舍五入”。

评标办法

分值构成(总分 100 分)			技术部分：65 分； 综合部分：35 分；
条款号	**评分因素**	**分值**	**指标说明及评分标准**
（1）	技术部分（65 分）	技术指标响应程度（25分）	1、根据供应商提供技术偏离情况和证明文件打分，全部满足招标文件技术规格要求得25分。 2、 “★”条款为重要指标，每有一项指标负偏离的扣1分；非“★”条款为一般性指标，每有一项指标负偏离的扣0.5分，25分扣完为止。 注：未按要求提供相关证明材料按负偏离进行扣分。
		技术方案（15 分）	根据各投标人对本项目的技术实施方案，分析项目需求，包含安全服务内容、范围、质量控制、风险控制；分别提供云安全和商用密码应用的技术方案。方案内容完整，且没有缺项得 15 分。未提供方案或缺项不得分。
		项目团队服务能力（10 分）	1、投标人提供本项目服务团队负责人同时具有 CISP、CISAW、CISP-DSG 认证证书的得 3 分。 2、投标人提供针对本项目实施工程师技术服务团队；团队成员具有CISP、CISP-PTE或CISP-DSG认证证书，每提供一人得0.5分，最多得3分； 3、投标人提供不少于 2 人的项目驻场服务团队，团队中至少 2 人具备 CISP 认证证书的得 2 分。 4、为保障商用密码服务能力，提供厂商为本项目配备的密码技术负责人，具备信息系统项目管理师证书、注册信息安全专业人员 CISP 证书或数据安全人员能力认证证书其中两项资质证书的得 2 分。
		售后服务方案及技术培训方	各投标人对本项目提供详细的售后服务方案及技术培训方案，技术培训内容需包含本项目涉及的所有产品和技术培训内容。售后服务在满足采购人要求的基础上提供

		案（10 分）	项目的服务计划和服务方案。方案内容完整，且没有缺项得 10 分。未提供方案或缺项不得分。
		驻场运维方案（5 分）	提供详细的驻场运维服务方案，服务方案在满足采购人要求的基础上提供项目的服务计划和服务内容。方案内容完整，且没有缺项得 5 分。未提供方案或缺项不得分。
（2）	综合部分（35 分）	企业实力（15 分）	1、投标人提供 ISO/IEC 20000-1：2018 标准信息技术服务管理体系认证证书的（附证书扫描件加盖公章），得 2 分，不提供的不得分。 2、投标人提供 GB/T 22080-2016/ISO/IEC 27001:2022 标准信息安全管理体系认证证书（附证书扫描件并加盖公章），得 1 分，不提供的不得分。 3、投标人具有信息安全风险评估服务资质的得 2 分。（附资质证书扫描件并加盖公章，不提供的不得分。） 4、投标人具有信息安全工程类证书的得 1 分。（附资质证书扫描件并加盖公章，不提供的不得分。） 5、投标人具有 CCRC 信息系统安全集成资质证书、信息安全风险评估资质证书、信息安全应急处理资质证书、安全运维资质证书，证书齐全的，得 4 分，每缺一项扣 1 分。（附资质证书扫描件并加盖公章，不提供的不得分。） 6、投标人具有 CNNVD 或 CNVD 技术支撑单位等级证书的，一级得 2.5 分，2 级得 1.5 分，3 级得 1 分，没有不得分。（附资质证书扫描件并加盖公章，不提供的不得分。） 7、投标人结算金额折扣率每降 1%加 0.5 分，最多加 2.5 分。
		厂商实力（9 分）	1、为满足要求，云安全资源池厂商参与信息安全等级保护关键技术国家工程实验室建设，并提供证明文件复印件得 2 分，不提供的不得分。

			2、为保证产品漏洞发现能力，云安全资源池厂商向国家信息安全漏洞共享平台(CNVD 或 CNNVD)报送原创漏洞信息数量不少于 60000 条，制造商需提供近两年内漏洞报送证明复印件得 1 分，不提供的不得分。 3、为保障信息化建设及服务能力，云安全资源池厂商具备 CIC 信息化建设及数字化能力评价一级证书，能够提供复印件得 1 分，不提供的不得分。 4、为保证产品数据服务安全性，云安全资源池厂商具备 CNAS 认证的 DSMM 数据安全能力成熟度认证 3 级及以上证书，能够提供证书复印件得 1 分，不提供的不得分。 5、为保证软件开发方的技术能力、管理能力以及软件开发能力生命周期全过程等方面开发能力，云安全资源池厂商具备 CCRC 信息安全服务软件安全开发一级资质,提供证书复印件得 1 分，不提供的不得分。 6、为保证商用密码服务能力，密码厂商需具备良好的软件业务能力，具有 CMMI 认证或 CSMM 认证，且具有 CMMI 三级及以上或 CSMM 三级及以上认证证书的得 1 分(提供证书复印件）。 7、为保证商用密码安全水平，密码厂商同时具备国家信息安全工程类测评信息安全服务资质证书和 CCRC 信息安全服务资质认证证书（信息系统安全集成）的得 2 分（提供证书复印件）。
		业绩（6 分）	投标人提供 2022 年 1 月 1 日以来类似项目合同案例，每提供一份得 2 分，最多得 6 分。 （提供合同原件扫描件，以合同签订时间为准，未提供者不得分）
		勘察证明（5 分）	为保证方案的可行性和适配性，投标人提供采购人出具的实地勘察证明扫描件的得 5 分，不提供的不得分。

注：评标结束后，由采购人对评审结果及响应文件等进行复核，并在法定的时间内确定中标人。

1、依据中华人民共和国财政部令第 87 号令《政府采购货物和服务招标投标管理办法》第三十一条要求，不同投标人所投核心产品对应品牌完全相同且通过资格审查、符合性审查的，将按照一家投标人计算。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，按照除价格分外得分最高（商务+技术参数）的同品牌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。

2、按照周口市交易中心规定，本项目投标人所需提供原件在评标时无需提供，仅作为采购单位核实时使用，评审委员会评审时仅以投标人投标文件中扫描件为准。

第十条 评委独立评审后，评委会对投标人某项指标如有不同意见，按照少数服从多数的原则，确定该项指标是否通过。

第十一条 商务、技术满足招标文件要求，综合得分最高的投标人将作为中标候选人。如果综合得分中出现两家或两家以上相同者，投标报价较低者优先中标，报价也相同的，由采购人自行确定。

第十二条 评委会在评标过程中发现的问题，应当及时作出处理或者向采购人提出处理建议，并作书面记录。

第十三条 评标后，评委会应填写评审记录并签字。评审记录是评委会根据全体评标成员电子签字的原始评标记录和评标结果编制的报告，评委会全体成员均须在评审纪要上电子签字。评审记录应如实记录本次评标的主要过程，全面反映评标过程中的各种不同的意见，以及其他澄清、说明、补正事项。

三．评标纪律

第十四条 评委会和评标工作人员应严格遵守国家的法律、法规和规章制度；严格按照本次招标文件进行评标；公正廉洁、不徇私情，不得损害国家利益；保护招、投标人的合法权益。供应商不得相互串通投标报价，不得妨碍其他供应商的公平竞争，不得损害采购人或其他供应商的合法权益。供应商不得以向采购人、评委会成员行贿或者采取其他不正当手段谋取中标。

第十五条 在评标过程中，评委必须对评标情况严格保密，任何人不得将评标情况透露给与投标人有关的单位和个人。如有违反评标纪律的情况发生，将依据《中华人民共和国政府采购法》及其他有关法律法规的规定，追究有关当事人的责任。

第十六条 在招标采购中，出现下列情形之一的，应予废标：

1.出现影响采购公正的违法、违规行为的。

2.投标时有弄虚作假的行为。

第十七条 在投标过程中，出现下列情况之一的，按照无效投标处理：

1.未按照招标文件规定要求签署、签章的**（目前，周口市公共资源电子交易平台为每个投标单位只办理了两个 CA 证书，一个用于单位投标和签章，一个用于法定代表人签章。所以，在投标文件需要电子签章时，投标单位签投标单位电子章，法定代表人签法定代表人电子章；法定代表人有授权代表投标时，出具授权委托书，授权代表的名字直接打印在签章处即可）；**

2.不具备招标文件中规定资格要求的；

3.不符合法律、法规和招标文件中规定的其他实质性要求的。

4.投标人的报价超过了采购预算，采购人不能支付的；

5.投标文件附有招标人不能接受的条件；

6.投标文件中对同一服务或标段提供选择性报价的；

7.商务偏差表或技术偏差表存在弄虚作假的；

8.不同供应商的电子投标（响应）文件上传计算机的网卡 MAC 地址、CPU 序列号和硬盘序列号等硬件信息相同的;

9.不同供应商的投标（响应）文件由同一电子设备编制，打印、复印、加密或者上传的；

10.不同供应商的投标（响应）文件由同一人送达或者分发，或者不同供应商联系人为同一人或不同联系人的联系电话一致的；

11.不同供应商的投标（响应）文件的内容存在两处以上细节错误一致；

12.不同供应商的法定代表人、委托代理人、项目经理、项目负责人等由同一个单位缴纳社会保险或者领取报酬的；

13.不同供应商投标（响应）文件中法定代表人或者负责人签字出自同一人之手。

14. 有关证明的复印件/扫描件均需加盖公章，供应商提交的资料应签署“与原件一致”字样。

第十八条 在投标文件中，出现下列情形之一的，其投标有可能被拒绝：

1.服务工期不确切、不肯定的投标；

2.对售后服务、付款方式不满足招标文件要求的；

3.投标人没有实质性响应招标文件的要求和条件的；

4.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的；且提供的书面说明和相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

第十九条 本评标办法的解释权属于采购人。

招标文件第二部分

第五章 投标人须知

一. 总　　则

1.适用范围

1.1 本招标文件仅适用于本次公开招标所述的服务项目采购。

2.有关定义

2.1 招标人（采购人）：周口日报社。

2.2 招标代理机构（集中采购机构）：系指周口市公共资源交易中心政府采购中心，以下简称“采购中心”。

2.3 政府采购监督管理部门：系指周口市财政局政府采购监督管理科。

2.4 投标人：系指已经在周口市公共资源交易中心网上下载招标文件的投标人，且已经提交或准备提交本次投标文件的制造商、供应商或服务商。

2.服务：系指本项目所采购内容。

2.6 业绩：系指符合本招标文件规定且已供货（安装）完毕的合同及相关证明。

2.7 投标人公章：在电子投标文件中系指投标人电子签章。

3.投标费用

3.1 无论投标结果如何，投标人应自行承担其编制与递交投标文件所涉及的一切费用。供应商应承诺无论本项目招标过程中的做法和结果如何，均承担因参加本次投标而产生的全部费用。**评标委员会评标费用由采购人支付。**

4.合格的投标人

4.1 合格的投标人应符合招标文件载明的投标资格。

4.2 投标人之间如果存在下列情形之一的，不得同时参加同一标段（包别）或者不分标段（包别）的同一项目投标：

4.2.1 法定代表人为同一个人的两个及两个以上法人；

4.2.2 母公司、全资子公司及其控股公司；

4.2.3 参加投标的其他组织之间存在特殊的利害关系的；

4.2.4 法律和行政法规规定的其他情形。

5.勘察现场

5.1 本项目需要勘察现场，各投标人于招标公告截止后的第一个工作日与采购人联系（联系人：张峰　联系电话：18639402169），进行现场勘察。投标人可根据投标需要自行对供货现场和周围环境进行勘察，以获取编制投标文件和签署合同所需的资料。

5.2 勘察现场所发生的费用由投标人自行承担。采购人向投标人提供的有关供货现场的资料和数据，是采购人现有的能使投标人利用的资料。采购人对投标人由此而做出的推论、理解和结论概不负责。投标人未到供货现场实地踏勘的，中标后签订合同时和履约过程中，不得以不完全了解现场情况为由，提出任何形式的增加合同价款或索赔的要求。

5.3 除非有特殊要求，招标文件不单独提供供货使用地的自然环境、气候条件、公用设施等情况，投标人被视为熟悉上述与履行合同有关的一切情况。

5.4 投标人须承诺：因未勘察现场而给自己造成的损失，跟采购人无关，并不得以不完全了解现场情况为由，增加合同价款或索赔的要求。

6.知识产权

6.1 投标人须保证，采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，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或经济纠纷。如投标人不拥有相应的知识产权，则在投标报价中必须包括合法获取该知识产权的一切相关费用。如因此导致采购人损失的，投标人须承担全部赔偿责任。

6.2 投标人如欲在项目实施过程中采用自有知识成果，须在投标文件中声明，并提供相关知识产权证明文件。使用该知识成果后，投标人须提供开发接口和开发手册等技术文档。

7.纪律与保密

7.1 投标人应承诺其投标行为应遵守中国的有关法律、法规和规章。

7.2 投标人需保证不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评委会成员行贿或者采取其他不正当手段谋取中标。

7.2.1 有下列情形之一的，属于投标人相互串通投标：

7.2.1.1 不同投标人的投标文件由同一单位或者个人编制；

7.2.1.2 不同投标人委托同一单位或者个人办理投标事宜；

7.2.1.3 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；

7.2.1.4 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；

7.2.1.5 不同投标人的投标文件相互混装。

7.3 在确定中标人之前，投标人不得与采购人就投标价格、投标方案等实质性内容进行谈判，也不得私下接触评委会成员。

7.4 在确定中标人之前，投标人试图在投标文件审查、澄清、比较和评价时对评委会、采购人和采购中心施加任何影响都可能导致其投标无效。

7.5 由采购人向投标人提供的图纸、详细资料、样品、模型、模件和所有其它资料，被视为保密资料，仅被用于它所规定的用途。除非得到采购人的同意，不能向任何第三方透露。开标结束后，应采购人要求，投标人应归还所有从采购人处获得的保密资料。

7.6 供应商须出具自觉抵制政府采购领域商业贿赂行为承诺书；

8.联合体投标

不接受联合体投标，供应商需出具非联合体投标的声明函。

9.投标品牌

9.1 招标文件中提供的参考商标、品牌或标准（包括工艺、材料、设备、样本目录号码、标准等），是采购人为了方便投标人更准确、更清楚说明拟采购货物、服务的技术规格和标准，并无限制性。投标人在投标中若选用替代商标、品牌或标准，应优于或相当于参考商标、品牌或标准。

10.投标专用章的效力

10.1 招标文件中明确要求加盖电子签章的，投标人必须加盖投标人电子签章。

11.合同标的转让

11.1 合同未约定或者未经采购人同意，中标人不得向他人转让中标项目，也不得将中标项目肢解后分别向他人转让。供应商需对此作出承诺。

11.2 合同约定或者经采购人同意，中标人可以将中标项目的部分非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。如果本项目允许分包，采购人根据采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作交由他人完成的，应在投标文件中载明。

11.3 中标人应当就分包项目向采购人负责，接受分包的人就分包项目承担连带责任。

11.4 未经政府采购管理部门批准，进口设备不得转包。

12.会员信息库

12.1 为进一步规范招投标行为，提高招投标工作效率，降低投标成本，加强对投标人诚信信息的管理，加快周口市招投标工作电子化、信息化建设，为周口市公共资源交易

中心实行网上招投标奠定基础，经周口市公共资源交易管理办公室研究决定，周口市公共资源交易中心实行投标人会员信息库制度，并面向全国免费征集注册投标企业会员。

12.2 入库资料的真实性、有效性、完整性、准确性、合法性及清晰度由投标人负责。周口市公共资源交易中心只负责对投标人所提供的入库资料原件与上传扫描件进行比对；本项目所需会员库资料有效性由本项目评委会负责审核。各投标人须保证所提供的全部资料的真实性、合法性，否则其投标文件将作为无效处理。

为确保投标文件通过评审，投标人应及时对入库资料进行补充、更新。

如因前款原因未通过本项目评委会评审，由投标人承担全部责任。

12.3 网上会员库中文字资料与扫描件资料不一致时，以扫描件资料为准。

12.4 有关会员库的更多信息，请登陆周口市公共资源交易中心网查询。

13.采购信息的发布

13.1 与本次采购活动相关的信息，将发布在周口市公共资源交易中心网(http://jyzx.zhoukou.gov.cn)及河南省政府采购网（www.hngp.gov.cn），以下简称“网站”。

二．招标文件

14.招标文件构成

14.1 招标文件包括以下部分：

14.1.1 第一章：投标邀请（招标公告）；

14.1.2 第二章：投标人须知前附表；

14.1.3 第三章：需求一览表；

14.1.4 第四章：评标办法；

14.1.5 第五章：投标人须知；

14.1.6 第六章：采购合同；

14.1.7 第七章：投标文件格式；

14.1.8 周口市公共资源交易中心政府采购中心发布的图纸、答疑、补遗、补充通知等。

14.2 投标人应认真阅读招标文件中所有的事项、格式、条件、条款和规范等要求。

14.3 投标人应当按照招标文件的要求编制投标文件。投标文件应对招标文件提出的要求和条件作出实质性响应。

14.4 投标人获取招标文件后，应仔细检查招标文件的所有内容，如有残缺等问题应在获得招标文件 3 日内向周口市公共资源交易中心政府采购中心或采购人提出，否则，由此引起的损失由投标人自行承担。

15.招标文件的澄清与修改

15.1 周口市公共资源交易中心政府采购中心或采购人对招标文件进行的澄清、更正或更改，将在网站上及时发布，该公告内容为招标文件的组成部分，对投标人具有同样约束力。澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构在投标截止时间至少 15 日前，将在网站上及时发布通知所有获取招标文件的潜在投标人；不足 15 日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。投标人应主动上网查询。周口市公共资源交易中心政府采购中心或采购人不承担投标人未及时关注相关信息引发的相关责任。

15.2 在投标截止时间前，采购人可以视采购具体情况，延长投标截止时间和开标时间，并在招标文件要求提交投标文件的截止时间三日前，在网站上发布变更公告。在上述情况下，采购人和投标人在投标截止期方面的全部权力、责任和义务，将适用于延长后新的投标截止期。

15.3 特殊情况下，采购人发布澄清、更正或更改公告后，可不改变投标截止时间和开标时间。

三．投标文件的编制

16.投标文件构成与格式

16.1 投标文件是对招标文件的实质性响应及承诺文件。

16.2 除非注明“投标人可自行制作格式”，投标文件应使用招标文件提供的格式。

16.3 除专用术语外，投标文件以及投标人与采购人就有关投标的往来函电均应使用中文。投标人提交的支持性文件和印制的文件可以用另一种语言，但相应内容应翻译成中文，对不同文字文本投标文件的解释发生异议的，以中文文本为准。

16.4 除非招标文件另有规定，投标文件应使用中华人民共和国法定计量单位。

16.5 除非招标文件另有规定，投标文件应使用人民币填报所有报价。允许以多种货币报价的，应当按照中国银行在开标日公布的汇率中间价换算成人民币。

16.6 投标文件应编制目录及连续页码，除特殊规格的图纸或方案、图片资料等外，均应按 A4 规格制作。

16.7 电报、电话、传真形式的投标概不接受。

16.8 电子投标文件制作，见周口市公共资源交易中心网站下载中心版块《投标单位-电子投标文件视频制作手册》的相关规定。

17.报价

17.1 投标人应以“包”为报价的基本单位。若整个需求分为若干包，则投标人可选择其中的部分或所有包报价。包内所有项目均应报价（免费赠送的除外），否则将导致投标无效。

17.2 投标人的报价应包含所投服务、保险、税费、包装、加工及加工损耗、运输、现场落地、安装及安装损耗、调试、检测验收和交付后约定期限内免费维保等工作所发生的一切应有费用。投标报价为签订合同的依据。

17.3 投标人应在投标文件中注明拟提供服务的单价明细和总价。

17.4 除非招标文件另有规定，每一包只允许有一个最终报价，任何有选择的报价或替代方案将导致投标无效。

17.5 采购人不建议投标人采用总价优惠或以总价百分比优惠的方式进行投标报价，其优惠可直接计算并体现在各项投标报价的单价中。

17.6 除政策性文件规定以外，投标人所报价格在合同实施期间不因市场变化因素而变动。

18.投标内容填写及说明

18.1 投标文件须对招标文件载明的投标资格、技术、资信、服务、报价等全部要求和条件做出实质性和完整的响应，并对所提供的全部资料做出真实性、合法性承诺，否则其投标文件将作为无效标处理。如果投标文件填报的内容资料不详，或没有提供招标文件中所要求的全部资料、证明及数据，将导致投标无效。

18.2 投标人应在投标文件中提交招标文件要求的有关证明文件（扫描或影印件上传），作为其投标文件的一部分。

18.3 投标人应在投标文件中提交（以扫描件或影印件上传）招标文件要求的所有服务的合格性以及符合招标文件规定的证明文件（可以是手册、图纸和资料）等，并作为其投标文件的一部分。包括：

18.3.1 服务主要性能（内容）的详细描述；

18.3.2 保证所投服务正常、安全、连续运行期间所需的所有备品、备件及专用工具的详细清单。

18.4 投标文件应编排有序、内容齐全、不得任意涂改或增删。如有错漏处必须修改，应在修改处加盖投标人电子公章。

19.投标保证金（免收）

20.投标有效期

20.1 为保证采购人有足够的时间完成评标和与中标人签订合同，规定投标有效期。投标有效期期限见投标人须知前附表。

20.2 在投标有效期内，投标人的投标保持有效，投标人不得要求撤销或修改其投标文件。

20.3 投标有效期从投标截止日起计算。

20.4 在原定投标有效期满之前，如果出现特殊情况，采购人可以书面形式提出延长投标有效期的要求。投标人以书面形式予以答复，投标人可以拒绝这种要求而不被没收投标保证金。同意延长投标有效期的投标人不允许修改其投标文件的实质性内容，且需要相应地延长投标保证金的有效期。

21.投标文件份数和签署

21.1 投标人应按照投标人须知前附表的要求准备投标文件。

21.2 投标文件均应依招标文件要求加盖投标人电子签章。

四．投标文件的递交

22.投标文件的密封和标记

加密的电子投标文件的递交，见周口市公共资源交易中心网站下载中心版块《投标单位-电子投标文件视频制作手册》的相关规定。

23.投标文件的递交

23.1 投标人应当在招标文件要求提交投标文件的截止时间前网上投标。

23.2 在招标文件要求提交投标文件的截止时间之后制作上传的投标文件为无效投标文件，采购人将拒绝接收。

24.投标文件的修改和撤回

投标截止日期前，投标人可以修改或撤回其投标文件；在投标截止时间后，投标人不得再要求修改或撤回其投标文件。

五．开标与评标

25.开标

25.1 本项目实行网上远程开标无须到现场提交投标文件。投标文件提交及解密详见周口市公共资源交易中心网办事指南《不见面开标远程在线解密会员端操作手册操作指南》。

25.2 开标时，各投标单位应在规定时间内对本单位的投标文件现场解密。在解密投标文件开始时 30 分钟内进行解密，超时视为放弃递交投标文件。

25.3 投标资格及投标文件的法律文本将由评审委员会在评标前进行审查。资格不符合招标文件要求和相关法律规定的，投标无效。

25.4 开标时，周口市公共资源交易中心政府采购中心将通过网上开标系统公布投标人名称、投标价格，以及周口市公共资源交易中心政府采购中心认为合适的其它详细内容。

25.5 在评审结束前，未得到周口市公共资源交易中心政府采购中心允许，投标人授权代表不得离开开标现场。

26.投标文件的澄清、说明或补正

26.1 为有助于投标的审查、评价和比较，评标委员会可以书面方式要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容作必要的澄清、说明或补正。澄清、说明或补正不得超出投标文件的范围或改变投标文件的实质性内容。

26.2 投标文件中大写金额和小写金额不一致的，以大写金额为准；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；单价金额小数点有明显错位的，应以总价为准，并修改单价。

26.3 开标一览表内容与投标文件中明细表内容不一致的，以开标一览表为准。

26.4 如同时出现 26.2 条和 26.3 条所述的不一致情况，以开标一览表为准。

27.评标

27.1 评委会将按照招标文件规定的评标办法对投标人独立进行投标评审。投标评审分为符合性审查和综合评分。

27.2 符合性审查时，评委会将首先审查投标文件是否实质上响应招标文件的各项指标要求。实质上响应的投标应与招标文件的全部条款、条件和规格相符，没有重大偏离或保留。所谓重大偏离或保留是指影响合同的供货范围、质量和性能等；或者在实质上与招

标文件不一致，而且限制了合同中买方的权利或投标人的义务。这些偏离或保留将会对其他实质上响应要求的投标人的竞争地位产生不公正的影响。投标人不得通过修改或撤销不合要求的偏离或保留而使其投标成为响应性的投标。

有下列情形之一的，评标委员会应当否决其投标：

27.2.1 投标文件未经投标单位电子签章的；

27.2.2 投标联合体没有提交共同投标协议；

27.2.3 投标人不符合国家或者招标文件规定的资格条件；

27.2.4 同一投标人提交两个以上不同的投标文件或者投标报价，但招标文件要求提交备选投标的除外；

27.2.5 投标报价或者某些分项报价明显不合理或者低于成本，有可能影响商品质量和不能诚信履约；

27.2.6 投标报价高于招标文件设定的最高投标限价；

27.2.7 投标文件没有对招标文件的实质性要求和条件作出响应；

27.2.8 投标人有串通投标、弄虚作假、行贿等违法行为；

27.2.8 不同投标人在同一台计算机上制作投标文件的；

27.3 如果投标文件未通过投标符合性审查，投标无效。

27.4 评委会决定投标文件的响应性及符合性只根据投标文件本身的内容，不寻求其他外部证据。

28.废标处理

28.1 在招标采购中，出现下列情形之一的，周口市公共资源交易中心政府采购中心有权宣布废标：

28.1.1 符合专业条件的投标人或对招标文件作实质响应的投标人不足三家的；

28.1.2 投标人的报价均超过采购预算，采购人不能支付的；

28.1.3 出现影响采购公正的违法、违规行为的；

28.1.4 因重大变故，采购任务取消的。

废标后，周口市公共资源交易中心政府采购中心会把废标理由通知所有投标人。

28.2 因上条第一款、第二款规定情形导致废标的，若采购人提出申请，报经政府采购监督管理部门批准，可现场改为竞争性谈判，投标人有下列情形之一的，不得参加谈判：

28.2.1 放弃参加投标的；

28.2.2 未经周口市公共资源交易中心政府采购中心允许，离开开标现场通知不上的；

28.2.3 不符合招标文件列明的专业条件的；

28.2.4 未按规定交纳谈判保证金的；

28.2.5 有影响采购公正的违法、违规行为造成项目废标的；

28.2.6 其他不符合竞争性谈判条件的情况。

28.3 采购方式现场改为竞争性谈判时，周口市公共资源交易中心政府采购中心以《招标流标现场转谈判邀请函》方式函告投标现场各投标人，投标人授权代表签字确认参加谈判。放弃谈判的视同自动放弃本项目的投标资格。竞争性谈判应当至少有两家及以上投标人参加。如参加谈判的投标人少于两家，谈判做流标处理。

28.3.1 谈判时，若投标人未能在评委会指定时间内（原则上不超过 60 分钟）提交符合要求的补充资料或未作出实质性响应的，投标无效。经过审查符合谈判要求的有效投标人少于两家的，谈判做流标处理。

28.3.2 投标文件的报价视为谈判时的首次报价，未唱标转谈判的，谈判时不公开投标人各轮报价。已经唱标而转谈判的，谈判前公布各参与谈判的投标人首轮报价。

28.3.3 在谈判内容不作实质性变更及重大调整的前提下，投标人次轮报价不得高于上一轮报价。

29.二次采购

项目废标后，周口市公共资源交易中心政府采购中心可能发布二次公告（投标邀请），进行二次采购。

前款所述“二次”，系指项目废标后的重新公告及采购，并不仅限于项目的第二次公告及采购。

六．定标与签订合同

30.定标

30.1 投标符合性审查后，评委会应当按招标文件规定的综合评分办法提出独立评审意见，推荐中标候选人。

30.2 采购人应当自收到评审报告之日起 5 个工作日内在评审报告推荐的中标或者成交候选人中按顺序确定中标或者成交供应商。

30.3 如评委会认为有必要，首先对第一中标候选人就投标文件所提供的内容是否符合招标文件的要求进行资格后审。资格后审视为本项目采购活动的延续，以书面报告作为最终审查的结果。如果确定第一中标候选人无法履行合同，将按排名依次对其余中标候选

人进行类似的审查。

排名第一的中标候选人放弃中标、因不可抗力不能履行合同、不按照合同约定提交履约保证金，或者被查实存在影响中标结果的违法行为等情形，不符合中标条件的，采购人可以按照评标委员会提出的中标候选人名单排序依次确定其他中标候选人为中标人，也可以重新招标。

30.4 原则上把合同授予实质上响应招标文件要求的排名最前的中标候选人或通过上条资格审查的中标候选人。

30.5 最低报价并不是中标的保证。

30.6 凡发现中标候选人有下列行为之一的，其中标无效，并移交政府采购监督管理部门依法处理：

30.6.1 以他人名义投标、或提供虚假材料弄虚作假谋取中标的；

30.6.1.1 以他人名义投标，是指使用通过受让或者租借等方式获取的资格、资质证书投标。

30.6.1.2 有投标人有下列情形之一的，属于弄虚作假的行为：

30.6.1.2.1 使用伪造、变造的许可证件；

30.6.1.2.2 提供虚假的财务状况或者业绩；

30.6.1.2.3 提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；

30.6.1.2.4 提供虚假的信用状况；

30.6.1.2.5 其他弄虚作假的行为。

30.6.2 与采购人、其他供应商或者采购代理机构名称工作人员恶意串通的；

30.6.3 向采购人、评审专家、采购代理机构工作人员行贿或者提供其他不正当利益的；

30.6.4 有法律、法规规定的其他损害采购人利益和社会公共利益情形的；

30.6.5 其他违反招投标法律、法规和规章强制性规定的行为。

30.7 周口市公共资源交易中心政府采购中心将在政府采购相关网站上发布评审结果公告。

31.中标通知书

31.1 在发出中标公告后请采购人、中标人登录周口市公共资源交易中心网（http://jyzx.zhoukou.gov.cn）自行下载中标通知书。

31.2 周口市公共资源交易中心政府采购中心对未中标的投标人不做未中标原因的解

释。

31.3 评审结果确定后，中标人请及时到周口市公共资源交易中心政府采购中心领取中标通知书。

32.中标服务费

本项目免收中标服务费

33.履约保证金

无

34.签订合同

34.1 中标人应在中标通知书发出之日起 1 日历日内（具体时间、地点见中标通知书）与采购人签订合同。招标文件、中标人的投标文件及澄清文件等，均作为合同的附件。

34.2 采购双方必须严格按照招标文件、投标文件及有关承诺签订采购合同，不得擅自变更。合同的标的、价款、质量、履行期限等主要条款应当与招标文件和中标人的投标文件的内容一致，招标人和中标人不得再行订立背离合同实质性内容的其他协议。对任何因双方擅自变更合同引起的问题周口市公共资源交易中心政府采购中心概不负责，合同风险由双方自行承担。

34.3 采购人保留以书面形式要求合同的卖方对其所投服务的装运方式、交货地点及服务细则等作适当调整的权利。

35.验收

由采购人自行组织对供应商的履约验收。

36.质疑

36.1 投标人认为采购过程、中标结果使自己的合法权益受到损害的，可以在知道或应当知道自己的权益受到损害之日起 7 个工作日内，由投标人授权代表（或法人代表）按照相关规定，向采购人提出质疑，逾期不予受理。

36.2 质疑书内容应包括质疑的详细理由和依据，并提供有关证明资料。

36.3 有以下情形之一的，视为无效质疑：

36.3.1 未按规定时间或规定手续提交质疑的；

36.3.2 质疑内容含糊不清、没有提供详细理由和依据，无法进行核查的；

36.3.3 其他不符合质疑程序和有关规定的。

被判定无效质疑的，采购人将书面回复投标单位其质疑无效的理由，并记录无效质疑一次。

36.4 采购人将在受到书面质疑后 7 个工作日内审查质疑事项，作出答复或相关处理决定，并以书面形式通知质疑人，但答复的内容不涉及商业秘密。

36.5 投诉人有下列情形之一的，属于虚假、恶意投诉，政府采购监督管理部门将驳回投诉，将其列入不良行为记录名单，并依法予以处罚：

36.5.1 一年内三次以上投诉均查无实据的；

36.5.2 捏造事实、提供虚假投诉材料或提供以非法手段取得的证明材料质疑的；

36.5.3 其他经认定属于虚假、恶意投诉的行为。

37.未尽事宜

37.1 按《中华人民共和国政府采购法》及其他有关法律法规的规定执行。

38.解释权

38.1 本招标文件的解释权属于采购人。

第六章

周口市政府采购合同（服务类）标准文本

政府采购项目名称：

政府采购项目编号：

采　　购　　人：

供　　应　　商：

合　同　签 订 地：

合 同 签订 时 间：

合同签订指引

一、采购人在签订合同时应提供的资料：

1、该政府采购项目的招标采购文件（以网上发布内容为准）；

2、该政府采购项目招标文件的澄清和修改内容（公告内容）；

3、该政府采购项目评审报告；

4、采购单位法人授权委托书（法人到场并签字的除外）；

5、采购单位被授权人身份证件（法人到场并签字的除外）；

6、采购人和中标供应商（或服务商，下同）约定的其它内容（不得超出招标采购文件实质性内容）。

二、供应商在签订合同时应提供的资料：

1、该政府采购项目的投标文件（纸质或 PDF 格式的电子投标文件）；

2、针对该项目评审时评审委员会提出的质询答复（纸质并签章）；

3、该政府采购项目中标通知书；

4、供应商法人授权委托书（法人到场并签字的除外）；

5、供应商被授权人身份证件（法人到场并签字的除外）；

6、供应商和采购人约定的其它内容（不得超出招标采购文件实质性内容）。

三、本合同签订后一个工作日内有采购人在“周口市政府采购网”上进行合同公示。

供应商履约验收指引

1、供应商不得擅自变更合同标的服务内容；

2、不得以次充优，随意降低服务标准和水平；

3、对因客观上采购人采购需求发生变化造成的，应提供采、供双方的纸质备忘录材料；

4、在满足验收条件 5 个工作日内通知采购人组织验收；

5、供应商应提供需验收服务的清单、标准、达到的水平等量化资料；

6、采、供双方约定的验收机构及相关人员组成情况。

7、督促采购人在项目验收结束并达到相关要求后一个工作日内，在“周口市政府采购网”上进行“履约验收”公示。

服务合同内容

采购人（甲方）：

供应商（乙方）：

签订地点：

项目名称：

项目编号：

财政委托号：_____(财政资金项目必须填写)

本项目经批准采用 公开招标 采购方式，经本项目评审委员会认真评审，决定将采购合同授予乙方。为进一步明确双方的责任，确保合同的顺利履行，根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，经甲乙双方充分协商，特订立本合同，以便共同遵守。

第一条 服务的内容、标准、数量和价格：（若服务项目过多则见附表，如有附表则必须加盖印章）

服务内容	标准水平	单位	数量	单价	小计	备注
合同总价款（大小写）： 备注：上述服务包含相关设备购置、人员工资及售后服务、税金、劳保基金、人员培训等费用。						

第二条 服务标准（包括达到的水平要求），按下列第（① ）项执行：

①按国家标准执行；②按部颁标准执行；③若无以上标准，则应不低于同行业服务标准；④有特殊要求的，按甲乙双方在合同中商定的要求执行；

乙方提供的服务标准和水平应与招标采购文件规定的标准和水平相一致。

第三条 服务的方式、方法、地点和期限

1、服务方式：

2、服务方法：

2、服务地点：

3、服务期限：

第四条 费用及支付方式

㈠本项目费用有以下组成：

1、XX 万元；

2、XX 万元；

……

(二)费用支付方式：

1、XXXX；

2、XXXX ；

3、在支付前甲方对乙方的服务进行考核或验收，合格的支付相应款 项。乙方须向甲方出具合法有效完整的完税发票及凭证资料进行支付结算。

第五条　付款条件

本合同以人民币付款。

该项目是否实行预付款：

实行预付款的条件和比例：

合同款项结算方式和支付比例：

(具体付款方式按投标人须知前附表以及采、购双方的具体约定

第六条　验收方法

1.甲、乙双方应严格履行合同有关条款，如果验收过程中发现乙方在没有征得采购人同意的情况下擅自变更合同服务内容，将拒绝通过验收，由此引起的一切后果及损失由乙方承担。

2.甲方应承担项目验收的主体责任。项目验收时，应成立三人以上（由甲、乙双方、管理人员、技术人员、纪检等相关人员组成）验收小组，明确责任，严格依照采购文件、中标（成交）通知书、政府采购合同及相关验收规范进行核对、验收、签字形成验收结论，并出具书面验收报告。验收人员有不同意见的，按少数服从多数的原则，但在验收报告上应注明不同意见的内容。

3、甲方视情况可以邀请参加本项目的其他投标人或者第三方机构参与验收，参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。

4、涉及安全、消防、环保等其他需要由质检或行业主管部门进行验收的项目，必须邀请相关部门或相关专家参与验收。涉及社会化服务的项目，甲方将要求社会公众人员参与验收。

检测、验收费用承担方式：

第七条 知识产权

乙方应保证所提供的服务或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权。

第八条 无产权瑕疵条款

乙方保证所提供的服务的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。如有产权瑕疵的，视为乙方违约。乙方应负担由此而产生的一切损失。

第九条　履约（或质量）保证金

1.本项目不收取履约保证金。确需收取履约保证金的，甲方不得要求乙方以现款的形式提供。乙方提供的履约保证金按规定格式以银行保函形式提供，与此有关的费用由服务方承担。

2.若确需质量保证金的，质量保证金不得超过合同总价款的 5%

3.如乙方未能履行其合同规定的任何义务，甲方有权从履约保证金中取得补偿。

第十条 甲方的权利和义务

1、甲方有权对合同规定范围内乙方的行为进行监督和检查，拥有监管权。有权定期核对乙方提供服务所配备的人员数量。对甲方认为不合理的部分有权下达整改通知书，并要求乙方限期整改。

2、甲方有权依据双方签订的考评办法对乙方提供的服务进行定期考评。当考评结果未达到标准时，有权依据考评办法约定的数额扣除履约保证金。

3、负责检查监督乙方管理工作的实施及制度的执行情况。

4、根据本合同规定，按时向乙方支付应付服务费用。

5、国家法律、法规所规定由甲方承担的其他责任

第十一条 乙方的权利和义务

1、对本合同规定的委托服务范围内的项目享有管理权及服务义务。

2、根据本合同的规定向甲方收取相关服务费用，并有权在本项目管理范围内管理及合理使用。

3、及时向甲方通告本项目服务范围内有关服务的重大事项，及时配合处理投诉。

4、接受项目行业管理部门及政府有关部门的指导，接受甲方的监督。

5、国家法律、法规所规定由乙方承担的其它责任。

第十二条 违约责任

1、甲乙双方必须遵守本合同并执行合同中的各项规定，保证本合同的正常履行。

2、甲方逾期付款的，除应及时付足款项外，应向乙方偿付欠款总额万分之 /天的违约金；逾期付款超过 天的，乙方有权终止合同。

3、如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方对此均应承担全部的赔偿责任。

4、变更、中止或者终止合同，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

第十三条 转让与分包

1.除甲方事先书面同意外，乙方不得部分转让或全部转让其应履行的合同义务。

2.乙方应在投标文件中或以其他书面形式对甲方确认本合同项下所授予的所有分包合同。但该确认不解除乙方承担的本合同下的任何责任或义务。意即在本合同项下，乙方对甲方负总责。

第十四条 合同文件及资料的使用

1.乙方在未经甲方同意的情况下，不得将合同、合同中的规定、有关计划、图纸、样本或甲方为上述内容向乙方提供的资料透露给任何人。

2.除非执行合同需要，在事先未得到甲方同意的情况下，乙方不得使用前款所列的任何文件和资料。

第十五条 不可抗力事件处理

1.如果双方任何一方由于受诸如战争、严重火灾、洪水、台风、地震等不可抗力的事故，致使影响合同履行时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。不可抗力事故系指买卖双方在缔结合同时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事故。

2.甲乙双方的任何一方由于不可抗力的原因不能履行合同时，应及时向对方通报不能履行或不能完全履行的理由，在取得有关部门证明以后，允许延期履行、部分履行或者不履行合同，并根据情况可部分或全部免予承担违约责任。

第十六条 合同纠纷调处

1.按本合同规定应该偿付的违约金、赔偿金、保管保养费和各种经济损失，应当在明确责任后10天内，按银行规定的结算办法付清，否则按逾期付款处理。

2.本合同如发生纠纷，当事人双方应当及时协商解决，协商不成时，任何一方均可请本项目政府采购监督管理部门调解，调解不成，按以下第（ ）项方式处理：①根据《中华人民共和国仲裁法》的规定向**周口仲裁委员会**申请仲裁。②向合同签订地有级别管辖权的人民法院起诉。

3、甲、乙双方均有权利向本项目具有监管职能的政府采购监督管理部门举报反映对方在合同履约中的违法违纪行为。

第十七条 其他

下列关于周口市公共资源交易中心政府采购代理机构名称某项目（项目编号：某编号）的采购文件及有关附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：①招标文件；②乙方提供的投标文件；③服务承诺；④甲乙双方商定的其他文件。以上附件顺序在前的具有优先解释权。

本合同一式___份，甲乙双方各执___份，自双方当事人签字盖章之日起生效。

采购人（甲方）：　　（公章）　　供货人（乙方）：　　（公章）

地址：　　地址：

法定代表人：　　法定代表人：

委托代理人：　　委托代理人：

电话：　　电话：

开户银行：　　开户银行：

账号：　　账号：

_____年_____月_____日　　_____年_____月___日

第七章 投标文件格式

****项目

投

标

文

件

投标人：_____

_年_月_日

投标文件资料清单

序号	资料名称	页码范围
一	开标一览表	
二	投标人情况综合简介	
三	投标函	
四	投标分项报价表	
五	投标响应表	
六	服务质量承诺	
七	有关证明文件	
八	中小企业声明函	
九	售后服务	
十	所投服务的技术资料等	
十一	其他投标人认为需要提供得材料等	
十二	政府采购供应商诚信承诺书	
备注：投标文件资料清单是投标人制作投标文件的参考格式，并非必须格式，请各位投标人根据所投项目需要自行增减，是否依据了本格式或自行增减了多少格式并不是废标的条款。		

一．开标一览表

项目名称	
投标人全称	
投标范围	
1、最终投标报价（人民币）	1、投标报价：　　元、大写：
备注	折扣率：　　%

供应商名称：（电子签章）

授权委托人：

日期：　　年　月　日

二．投标人综合情况简介

(投标人可自行制作格式)

三．投标函

致：（采购人或采购代理机构）

根据贵方“（**项目名称、项目编号)**”项目招标邀请书或招标公告，正式授权下述签字人_____（姓名）代表投标人_____（投标人全称），提交规定形式的投标文件。

据此函，我方兹宣布同意如下：

（1）如我公司中标，愿意按招标文件规定提供交付服务（包括税费等工作）的总报价为人民币_____元，服务期_____。

（2）我方根据招标文件的规定，严格履行合同的责任和义务,并保证于买方要求的日期内完成服务，并通过买方验收。

（3）我方承诺报价低于同类货物和服务的市场平均价格。

（4）我方已详细审核全部招标文件，包括招标文件修改书（如有），参考资料及有关附件，我方正式认可本次招标文件，并对招标文件各项条款（包括开标时间）均无异议。我方知道必须放弃提出含糊不清或误解的问题的权利。

（5）我方同意从招标文件规定的开标日期起遵循本投标文件，并在招标文件规定的投标有效期之前均具有约束力。

（6)我方声明投标文件所提供的一切资料及周口市公共资源交易中心会员库申报资料均真实、及时、有效。由于我方提供资料不实而造成的责任和后果由我方承担。我方同意按照贵方提出的要求，提供与投标有关的任何证据、数据或资料。

（7）我方完全理解贵方不一定接受最低报价的投标。

（8）我方同意招标文件规定的付款方式。

（9）与本投标有关的通讯地址：_____

（10）本项目项目责任人：　　电话：

供应商名称：（电子公章）

法人代表：（签字）

日期：　　年　月　日

四．投标分项报价表

序号	名称	单位	数量	单价	小计	备注
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
	其他费用					
	合计					

供应商名称：（电子公章）

法人代表：（签字）

日期：　　年　月　日

备注：

报价为所投服务的单价组成。包括税金及其它。

五．投标响应表

按招标文件规定填写			按投标人所投内容填写	
第一部分：技术部分响应				
序号	品名	招标文件要求	投标响应	偏离说明
1				
2				
3				
4				
第二部分：资信及报价部分响应				
序号	内容	招标要求	投标承诺	偏离说明
1	服务期			
2	免费质保期			
3	付款响应			
4	业绩			
5	其他			

供应商名称：（电子公章）

法人代表：（签字）

日期：　　年　　月　　日

备注：

1、投标人必须逐项对应描述投标服务要求，如不进行描述，仅在响应栏填“响应”或未填写的，将可能导致投标无效；

2、投标人所投服务如与招标文件要求不一致，则须在上表偏离说明中详细注明。

3、响应部分可后附详细说明及技术资料，并应注明投标文件中对应的页码范围。

六．服务质量承诺

（投标人可自行制作格式）

七．有关证明文件

提供符合投标邀请（招标公告）、需求一览表及评标办法规定的相关证明文件。

八．中小企业声明函（工程、服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合 体中的中小企业、签订分包意向协议的中小企业）的具体情 况如下：

1.（标的名称），属于（采购文件中明确的所属行业）； 承建（承接）企业为（企业名称），从业人员___人，营业收入为___万元，资产总额为___万元，属于（中型企业、小型企业、微型企业）；

2.（标的名称），属于（采购文件中明确的所属行业）； 承建（承接）企业为（企业名称），从业人员____人，营业收入为___万元，资产总额为____万元，属于（中型企业、 小型企业、微型企业）； ……

以上企业，不属于大企业的分支机构，不存在控股股东 为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

注：1.从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2.本项目如是只面向中小企业采购的应当必须提供。

九．售后服务

（投标人可自行制作格式）

十. 所投服务的技术资料等

（投标人可自行制作格式，可附产品技术彩页）

十一. 其他投标人认为需要提供的材料等

十二. 政府采购供应商诚信承诺书

我公司自愿参与政府采购活动，严格遵守《中华人民共和国政府采购法》等相关法律法规的规定，坚守公平竞争，并无条件地遵守采购活动的各项规定，我们郑重承诺：如果在政府采购招标活动中有以下情形的,愿接受政府采购监管部门给予相关处罚并承担法律责任。

（一）提供虚假材料谋取中标;

（二）采取不正当手段诋毁、排挤其他供应商;

（三）与招标采购单位、其他投标人恶意串通;

（四）向招标采购单位或提供其他不正当利益;

（五）在招标过程中与招标采购单位进行协商谈判、不按照招标文件和投标文件订立合同，或者与采购人另立背离合同实质性内容协议;

（六）开标后擅自撤销投标，影响招标继续进行的或领取招标文件纳投标保证金后不投标导致废标;

（七）中标后无正当理由，在规定时间内不与采购单位签订合同;

（八）将中标项目转让给他人或非法分包他人;

（九）无正当理由，拒绝履行合同义务;

（十）无正当理由放弃中标（成交）项目;

（十一）擅自或与与采购人串通或接受采购人要求，在履约合同中通过减少服务数量，更服务标准等，却仍按原合同进行虚假验收或终止政府采购合同;

（十二）与采购人串通，对尚未履约完毕的采购项目出具虚假验收报告；

（十三）无不可抗力因素，拒绝提供售后服务、售后服务态度恶劣、故意提高维修配件价格（高于市场平均价）；

（十四）开标后对招标文件的相关内容再进行质疑；

（十五）恶意投诉的行为：投诉经查无实据的、捏造事实或者提供虚假设诉材料；

（十六）拒绝有关部门监督检查或者提供虚假情况；

（十七）政府采购监管部门认定的其他政府采购活动中的不诚信行为。

供应商名称：（电子公章）

法人代表或授权委托人：（签字）

日期：　　年　　月　　日

周口市政府采购合同融资政策告知函

各供应商：

欢迎贵公司参与周口市政府采购活动！

政府采购合同融资是河南省财政厅支持中小微企业发展，针对参与政府采购活动的供应商融资难、融资贵问题推出的一项融资政策。贵公司若成为本次政府采购项目的中标成交供应商，可持政府采购合同向金融机构申请贷款，无需抵押、担保，融资机构将根据《河南省政府采购合同融资工作实施方案》（豫财购〔2017〕10 号），按照双方自愿的原则提供便捷、优惠的贷款服务。

贷款渠道和提供贷款的金融机构，可在河南省政府采购网“河南省政府采购合同融资平台”查询联系。