

## 二、投标报价表

### 2.1 开标一览表

项目编号：ZDCG2026-001GK

单位：元

合同包名称	投标报价	服务期限	服务质量	服务地点	备注
合同包 2: 志丹县 全县政务网络整合 政府购买社会化 服务采购	13781660.00	本项目合同有效期： 自合同签订之日起 1 年。 本项目履行期限三年 (一次招标三年沿用)， 实行一年一考核一签 合同的办法，合同每 年签订一次。一年期 满后，采购人根据相 关政策以及成交供应 商服务质量与成交供 应商续签下一年合同 ，以本次采购内容及 报价为依据	满足采购需求及相 关技术要求	按采购人指定地点	
<b>投标总报价（元/年）：</b> （大写）：壹仟叁佰柒拾捌万壹仟陆佰陆拾元整（小写：¥13781660.00 元/年）					

说明：1. 投标报价应按项目总报价填写，精确到小数点后两位，大小写不一致时，以大写为准。

投 标 人：延安高度科技有限责任公司（盖单位章）

法定代表人（单位负责人）或委托代理人：刘佳（签名）

日 期：2026 年 2 月 12 日

## 2.2 分项报价表

一、网络服务						
序号	项目	内容	数量	单位	单价(元)	总价(元)
1	全县政务外网服务及运维管理	全县政务外网服务及运维管理, 用户数量4000, 网络出口数量: 3 个, 网络负载均衡, 用户流量管理	1	项	1950000	1950000
2	全县政务内网服务及运维管理	全县政务内网服务及运维管理, 20 个单位, 网络负载均衡, 用户流量管理	1	项	2242000	2242000
3	网络视频服务及运维管理	网络视频服务及运维管理, 10 单位高清视频会议, 网路稳定, 画面清晰	1	项	860000	860000
4	业务专网服务及运维管理	业务专网服务及运维管理, 8 单位业务专网服务, 网络负载均衡, 用户流量管理	1	项	650000	650000
5	云储存及运维管理	云储存及运维管理 配置描述: 容量: 100TB IOPS 最大: 7K 带宽最大: 150MB/s 时延: <100ms	1	项	345000	345000
6	云政务服务及运维管理	云政务服务及运维管理, 提供全面、综合的政务云服务框架, 将网络问政、市民论坛、市长信箱、民意征集、网上调查、网上评议、在线访谈等诸多互动、交流应用模块, 整合到一个体系内, 不仅能够健全政府职责, 完善公共服务, 更能大力推进电子政务服务化, 强化社会管理和公共服务, 建设服务型政府, 努力提高政府的执行力和公信力。	1	套	200000	200000
7	培育数字化示范场景	培育数字化示范场景	2	个	60000	120000
8	AC 控制器	1、性能要求: 转发能力 10Gbps, 最大可管理 AP 数量 512 个; 2、接口要求: 千兆电口 10 个, 万兆光口 2 个; 3、功能要求: 支持 4~7 层应用识别, 可识别 6000 多种应用, 包括 LYNC/Face time/YouTube/Facebook 等常见办公应用与 P2P 下载应用; 4、配置要求: WLAN 无线接入控制器 AP 资源授权数 170 个, 万兆多模光模块 2 个, 原厂硬件质保及软件升级服务 3 年。	2	台	35000	70000
9	24 口 POE 接入交换机	1、性能要求: 交换容量 670Gbps, 包转发率 220Mpps; 2、接口要求: 2.5GE 电接口 24 个, 全部支持 802.3at POE+功能, 万兆光口 4 个, 万	16	台	8550	136800

		兆堆叠专用口 2 个，POE 输出功率 1000W； 3、芯片要求：采用国产关键芯片(CPU)； 4、管理要求：支持统一用户管理功能，支持 802.1X/MAC 等多种认证方式，支持 1024 认证用户同时在线； 5、PoE 供电要求：交换机重启时（如软件版本升级时重启），对下挂 PD 设备供电不会中断，保证交换机重启过程中 PD 不掉电，实现 PoE 供电零中断。 6、配置要求：万兆单模光模块 2 个，原厂硬件质保 3 年。				
10	放装 AP	1、协议要求：支持 802.11be 标准； 2、射频要求：支持 2.4GHz/5GHz 双频段，总空间流数 4；整机速率 3.5Gbps； 3、芯片要求：采用国产化 Wi-Fi 芯片； 4、接口要求：2.5GE 电接口 1 个； 5、功能要求：支持 AP 零配置，AP 可以通过 DHCP、DNS 方式自动注册到无线控制器 AC； 6、配置要求：原厂硬件质保 3 年。	22	台	1250	27500
11	面板 AP	1、协议要求：支持 802.11be 标准； 2、射频要求：支持 2.4GHz/5GHz 双频段，总空间流数 4；整机速率 3.5Gbps； 3、芯片要求：采用国产化 Wi-Fi 芯片； 4、接口要求：2.5GE 电接口 1 个，千兆电口 5 个； 5、功能要求：支持 AP 零配置，AP 可以通过 DHCP、DNS 方式自动注册到无线控制器 AC； 6、配置要求：原厂硬件质保 3 年。	160	台	1150	184000
12	高密 AP	1、协议要求：支持 802.11be 标准； 2、射频要求：支持 2.4GHz/5GHz 双频段，总空间流数 6；整机速率 6.4Gbps； 3、芯片要求：采用国产化 Wi-Fi 芯片； 4、接口要求：2.5GE 电接口 1 个，千兆电接口 1 个； 5、功能要求：支持 AP 零配置，AP 可以通过 DHCP、DNS 方式自动注册到无线控制器 AC； 6、配置要求：原厂硬件质保 3 年。	5	台	1840	9200
13	数字政务服务	“刷脸即办”系统	1	套	155000	155000
14	OA 办公系统	智能公文、智能会议、智能督办、信息传达、机关审批、智能后勤、机关大脑、移动办公八大模块	1	套	385000	385000

15	数据接口服务	定制开发,6 单位业务系统数据读取接口开发	1	项	120000	120000
16	网络态势感知服务	性能参数: 吞吐量: 2Gbps。 硬件参数: 规格: 2U, CPU: 1 颗 5380 2.5G (16C), 内存: 2*32GB DDR4 3200, 系统盘: 1*480GB SATA SSD, 缓存盘: 无缓存盘, 数据盘: 3*4TB, 标配盘位数: 4, 电源: 白金, 冗余电源, 接口: 2 千兆电口+2 万兆光口。 功能描述: APT 威胁检测系统是以安全可视和协同防御为主线, 以全流量采集技术、AI 智能分析技术、威胁情报技术三大关键技术, 为客户打造一套智能化、精准化、高效化的全流量威胁分析系统。	1	台	352000	352000
17	用户上网行为管理	性能参数: 网络层吞吐量 (大包): 10Gb, 应用层吞吐量: 1.5Gb, 带宽性能: 1Gb, IPSEC VPN 加密性能 (最高性能): 200M, 支持用户数: 6000, 准入终端数 (支持客户端授权): 3000, 准入终端数的扩容上限 (支持客户端授权-需单独收费): 6000, 包转发率: 132Kpps, 每秒新建连接数: 14000, 最大并发连接数: 600000。 硬件参数: 规格: 2U, 内存大小: 8G, 硬盘容量: 960G SSD, 电源: 冗余电源, 接口: 6 千兆电口+4 千兆光口 SFP。 功能描述: 全网行为管理聚焦企事业组织网络行为安全, 实现全网资产、身份、行为可视可控, 智能感知内部威胁风险, 帮助用户构建有效防御体系。	1	台	245000	245000
18	防病毒管理	性能参数: 最大支持管控 aES 客户端数量: 1W 点。 安全策略模板一体化设置, 全网资产盘点与风险可视, 自动化日志可视化报表一键导出, 管理账号分权分域, 总分平台级联控制; 管理平台需搭配客户端软件一齐使用, 单独购买无效, 含 1 年升级维护费用 统一端点安全管理系统软件 V6.0 (产品控制中心), 每套含: 4000 套* 端点安全软件 V6.0 (PC 全量版); 3 年* 软件升级 (PC 端);	1	套	285500	285500
19	数字水务、数字应急、数字气象应用服务	定制开发, 3 单位视频系统平行会议系统开发	1	项	90000	90000
20	数字城管、数字交	定制开发, 4 单位数据融合共享系统开发	1	项	200000	200000

	警、数字教育、数字医疗融合服务					
21	智慧城市系统运维	7*24 小时*365 天全系统全设备运维保障	1	项	600000	600000
22	智慧园区数据对接服务	工业园区数据对接定制开发	1	项	200000	200000
23	工业园区自建光缆	48 芯	15000	米	13	195000
24	接入防火墙	<p>性能参数：网络层吞吐量：10G，应用层吞吐量：4G，防病毒吞吐量：1G，IPS 吞吐量：1G，全威胁吞吐量（不含 WAF）：800M，并发连接数：400 万，HTTP 新建连接数：10 万，SSL VPN 推荐用户数（单独购买）：150，SSL VPN 最大用户数（单独购买）：750，SSL VPN 最大理论加密流量（单独购买）：150M，IPSec VPN 最大接入数：1000，IPSec VPN 吞吐量：800M。</p> <p>硬件参数：规格：1U，内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6 千兆电口。</p> <p>AF-1000-L2100 标准产品，每台含：  1 套* 防火墙软件基础级；  3 套* 云智订阅软件（AF8.0.7 及以上版本适用）；  1 套 3 年* 云威胁情报网关订阅软件  3 年* 维保服务（标准版）；</p>	1	台	120000	120000
25	网络安全托管服务（政务版）	<p>安全托管服务（政务版）</p> <p>服务概述：  政务版的安全托管服务（Managed Security Service，简称：MSS）以保障用户网络安全“持续有效”为目标，将用户安全设备接入安全运营中心，围绕资产、脆弱性、威胁、事件四个要素，通过云端安全运营中心和安全专家团队有效协同的“人机共智”模式为用户扩展 7*24H 持续有效的安全运营能力，保障可承诺的风险管控效果。</p> <p>服务内容：  1、运营准备阶段  1.1 服务上线  组件部署与接入：安全专家对需要接入 MSS 的组件（如 TSS/SIP/AF/EDR 等）进行部署并接入至 MSSP 安全运营平台。  资产收集与录入：安全专家在上线前对服务</p>	1	套	160000	160000

	<p>资产进行收集,并将资产信息录入到安全运营平台中进行管理。</p> <p>1.2 安全现状评估</p> <p>策略检查:上线前安全专家对安全组件上的安全策略进行统一检查,确保安全组件上的安全策略始终处于最优水平,针对威胁能起到最好的防护效果。</p> <p>脆弱性评估:对操作系统、数据库、常见应用/协议、系统与 Web 漏洞进行漏洞扫描,弱口令扫描可实现信息化资产不同应用弱口令猜解检测,如:SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。</p> <p>资产暴露面梳理:安全专家在上线前使用扫描组件对资产开展暴露面探测,以梳理资产面向互联网的开放情况,快速发现违规暴露在互联网中的资产及存在的风险并进行协助处置,实现对暴露面资产可管可控,降低暴露面资产的风险。(本项服务根据客户实际业务情况按需提供)</p> <p>1.3 安全问题处置</p> <p>策略调优:安全专家根据安全威胁/事件分析的结果以及处置方式,对安全组件上的安全策略进行调整工作。</p> <p>脆弱性问题修复指导:针对内网脆弱性,安全专家分析研判后提供实际佐证材料,并给出修复建议。</p> <p>2、持续有效运营</p> <p>2.1 资产管理</p> <p>资产指纹探测:持续服务过程中安全专家每季度对资产进行指纹(操作系统、中间件、软件厂商等信息)探测,并对指纹信息进行确认与更新,确保深信服安全运营中心中资产指纹信息的准确性和全面性。</p> <p>资产变更管理:持续服务过程中安全专家每季度对资产进行存活性探测,当发现未存活资产或资产发生变更时,安全专家对变更信息确认与更新,确保深信服安全运营中心中资产信息的准确性和全面性。</p> <p>2.2 脆弱性管理</p> <p>漏洞扫描与验证:每季度针对服务资产的系统漏洞和 Web 漏洞进行全量扫描,并针对发现的 WEB 漏洞进行验证,验证 WEB 漏洞在已有的安全体系发生的风险及分析发生后可</p>				
--	--	--	--	--	--

	<p>造成的危害。</p> <p>漏洞修复优先级排序与通告: 基于漏洞扫描结果、资产重要性及漏洞的威胁情报, 对漏洞进行重要性排序, 确定修复的优先级; 并将最终结果通告给用户。</p> <p>漏洞可落地修复方案: 对漏洞进行分析并输出可落地的修复方案, 通过工单系统跟踪修复情况。</p> <p>漏洞复测与状态追踪: 对修复的漏洞进行复测, 及时更新漏洞工单的漏洞修复状态。</p> <p>弱口令分析与管理: 实现信息化资产不同应用弱口令猜解检测, 如: SMB、Mssql、Mysql、Oracle、smtp、VNC、ftp、telnet、ssh、mysql、tomcat 等。针对不同行业提供行业密码字典, 有针对性的进行内网弱口令检测。并将检测发现的问题通过工单系统跟踪修复状态。</p> <p>高可利用漏洞防护: 对有深信服防火墙的用户, 支持一键防护扫描组件发现的高可利用漏洞。</p> <p>(本项服务根据客户实际业务情况按需提供)</p> <p>2.3 威胁管理</p> <p>7*24H 威胁分析研判: 基于云端安全能力平台, 云端专家提供 7*24 小时的威胁监测: 依托于安全防护组件、检测响应组件和安全平台, 将海量安全数据脱敏, 包括漏洞信息、共享威胁情报、异常流量、攻击日志等数据, 经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析, 实时监测网络安全状态, 对安全告警和威胁进行分析研判, 并生成工单。</p> <p>7*24H 威胁通告: 安全专家将云端分析确认后的真实威胁、事件实时通过微信、邮件等方式向用户通告, 并提供处置建议。</p> <p>威胁影响面分析: 安全专家针对每一个真实的威胁和告警, 进行深度分析验证, 分析判断受影响范围及是否攻击成功, 将深度关联分析的结果通过服务群/邮件等方式告知用户。</p> <p>威胁协助处置: 安全专家针对分析结果提供对应的处置或加固建议 (如封锁攻击源、设置安全策略防护等措施), 并协助用户闭环。</p>					
--	--	--	--	--	--	--

	<p>威胁情报管理: 实时抓取互联网最新威胁情报与详细资产信息进行匹配, 对最新威胁情报进行通告与排查, 结合威胁情报, 安全专家排查是否对服务资产造成影响并通知用户, 及时协助进行安全加固。</p> <p>高级威胁狩猎: 安全专家每年可按需开展 1 次针对内/外网或特定业务系统及特定漏洞, 基于客户业务定制检测逻辑, 尽可能快地发现漏洞或攻击痕迹, 发现潜在的安全隐患和已失陷的主机/被钓鱼成功的员工/账号信息泄露等, 最大限度地降低攻击者造成的危害, 评估造成的损失等内容, 最终帮助客户验证风险并推动发现的问题和隐患进行闭环处理。(本项服务根据客户实际业务情况按需提供)</p> <p>策略检查: 每季度安全专家对安全组件上的安全策略进行统一检查, 确保安全组件上的安全策略始终处于最优水平, 针对威胁能起到最好的防护效果。</p> <p>策略调优: 每季度安全专家根据安全威胁/事件分析的结果以及处置方式, 按需对安全组件上的安全策略进行调整工作。</p> <p>2.4 事件管理</p> <p>安全事件调查与分析: 安全专家 7*24H 在线服务, 针对主机发生的安全事件开展调查分析和影响面分析, 对发生的安全事件进行人工鉴定和举证分析。</p> <p>安全事件处置与闭环: 对客户网络内服务资产爆发勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件, 利用一些工具和脚本对恶意文件、代码进行根除, 帮助客户快速恢复业务, 消除或减轻影响, 闭环事件工单。</p> <p>重大事件应急响应: 通过事件检测分析, 提供抑制手段, 降低入侵影响, 协助快速恢复业务。排查攻击路径、恶意文件、清除。还原攻击路径, 分析入侵事件原因, 提供安全事件溯源结果。结合现有安全防御体系, 指导用户进行安全加固、提供整改建议、防止再次入侵。</p> <p>(本项服务根据客户实际业务情况按需提供)</p> <p>3、7*24 小时服务团队</p> <p>专属服务经理: 为用户配置一名经验丰富的</p>				
--	--	--	--	--	--

	<p>安全专家作为专属服务经理。</p> <p>实时专家咨询: 安全专家对用户咨询或上报的安全问题进行及时响应并给出建议, 如主机加固建议咨询、安全事件处置建议咨询等。</p> <p>节假日值守: 安全值守专家进行 7*24 小时安全监测, 对发生的安全事件进行及时响应并在节假日期间每日进行值守总结, 在服务群发送值守总结快报。</p> <p>4、运营成果可视</p> <p>安全运营周报: 安全专家每周对服务资产进行安全运营情况的分析总结并输出《安全运营周报》。</p> <p>安全运营月报: 安全专家每月对服务资产及整体安全状况进行分析总结并输出《安全运营月报》。</p> <p>安全运营半年度汇报: 安全专家每半年总结阶段性安全运营情况并输出《半年度总结报告》发送给用户, 向用户进行远程总结汇报。</p> <p>安全运营年度汇报: 安全专家总结年度安全运营情况并输出《年度总结报告》发送给用户, 向用户进行总结汇报。</p> <p>用户 Portal: 可视化 portal 支持随时查看服务范围内业务资产安全状态。支持在线展示所有脆弱性、威胁、事件工单的处置进程和结果支持用户在线对服务 SLA 进行查阅和监督。</p> <p>服务交付物:</p> <ul style="list-style-type: none"> <li>《项目启动会 PPT》</li> <li>《首次安全风险分析报告》</li> <li>《漏洞举证报告》(按需)</li> <li>《漏洞清单》(按需)</li> <li>《应急响应报告》(按需)</li> <li>《威胁情报》</li> <li>《暴露面梳理清单》(按需)</li> <li>《威胁狩猎报告》(按需)</li> <li>《安全运营周报》</li> <li>《安全运营月报》</li> <li>《半年度总结汇报》</li> <li>《年度总结汇报》</li> </ul>				
小计 (元)	9902000				

## 二、电子政务网络设备

序号	产品名称	产品规格	数量	单位	单价(元)	总价(元)
1	出口防火墙	1、防火墙吞吐量 35Gbps，最大并发连接数 2000 万，每秒新建连接数 50 万； 2、千兆 Combo 接口 8，千兆电口 4，万兆光口 10； 3、配置电源 2，配置 4 个风扇，支持 3+1 冗余备份； 4、防火墙采用自主研发的关键芯片(CPU)（第三方实验室测试报告证明，提供报告截图并加盖厂商公章或投标专用章）； 5、支持基于 IP（IPv6）、MAC 地址，安全组，时间等字段进行安全策略规则的配置； 6、支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； 7、可识别应用层协议数量 6000 种； 8、支持 BFD 链路检测，支持 BFD 与 VRRP 联动实现双机快速切换，支持 BFD 与 OSPF 联动实现双机快速切换； 9、支持 SSL VPN 功能，支持国密和其他商用密码算法； 10、实配：双电源；240G SSD 硬盘、100 个 SSL VPN 授权数、三年（IPS、AV、URL）特征库授权；三年原厂维保；	1	台	445350	445350
2	核心交换机	1、采用高可靠的 CLOS 交换架构，主控引擎与交换网板物理分离，支持信元交换，无阻塞跨板转发 2、交换容量 1904 Tbps，包转发率 460800Mpps，整机主控引擎插槽 2 个，业务插槽 8 个，交换网板插槽 9 个 3、支持颗粒化电源，支持 M+N 电源冗余（AC 和 DC 均支持），电源插槽个数 10，为保证设备散热可靠性，要求设备支持模块化风扇框，可热插拔，当单个风扇框发生故障时，有其他风扇正常运行，保证设备散热，独立风扇框数 3； 4、设备 CPU、转发或交换芯片采用国产化芯片； 5、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6 6、支持 VXLAN 分布式网关，集中式网关，支持 BGP-EVPN， 7、支持 Macsec 国密算法； 8、支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 等队列调度方式 9、支持真实业务流的实时检测技术，实现对 IP 网络的精确丢包监控和快速故障定界能力，提供权威第三	1	台	348970	348970

		<p>方测试报告</p> <p>10、实际配置：配置双主控，4个交换网板，4个电源，96个万兆光口，48个千兆电口，三年原厂维保。</p>				
3	48口接入交换机	<p>1、交换容量330Gbps，包转发率108Mpps；</p> <p>2、千兆电口48个，万兆光口4个；</p> <p>3、支持Console接口1个；</p> <p>4、网络指示灯：支持独立的网络指示灯，可以快速感知设备是否联网、是否被云管纳管。设备上线，清晰可见；</p> <p>5、散热方式：风冷散热，智能调速；</p> <p>6、二层功能：支持4K VLAN，支持MAC地址16K；</p> <p>7、以太环网保护：支持 ERPS 以太环保护协议（G.8032）；支持 STP（IEEE 802.1d），RSTP（IEEE 802.1w）和 MSTP（IEEE 802.1s）协议；</p> <p>8、MTBF：MTBF（平均无故障时间）超过40年；</p> <p>9、业务口防雷：业务口防雷可达10KV；</p> <p>10、可用度：可用度满足99.999%的电信级可靠性要求</p>	32	台	6870	219840
4	24口接入交换机	<p>1. 交换容量336Gbps，包转发率108Mpps；</p> <p>2. 24个千兆电口，4个万兆SFP+光口</p> <p>3. 支持Console接口；</p> <p>4. 支持独立的网络指示灯，可以快速感知设备是否联网、是否被云管纳管。设备上线，清晰可见</p> <p>5. 支持MAC地址16K；支持4K VLAN，并提供官网链接及截图</p> <p>6. MTBF（平均无故障时间）超过70年，并提供官网链接及截图；</p> <p>7. 业务口防雷可达10KV；</p> <p>8. 支持SNMP v1/v2/v3, Telnet, RMON, HTTPS, Web</p>	60	台	4600	276000

		等方式进行管理和维护，并提供官网链接及截图				
5	立式机柜	高0.6米宽600深600,加厚10U	30	个	3550	106500
6	UPS电池组	<p>标称电压：标准单体为 12V。</p> <p>容量规格： 65Ah, 。</p> <p>通常设计寿命为 10年以上（在25℃环境下）。</p> <p>支持大电流瞬间放电，配合UPS应对负载启动冲击。</p> <p>自放电率：极低自放电，20℃室温下储存，28天自放电率小于2%，</p> <p>存放两年后容量仍能保持较高水平。</p> <p>安全标准：外壳通常采用 UL94 V-0 级防火阻燃材料，具备防漏液、防酸雾设计。</p>	32	块	1350	43200
7	七氟丙烷药剂		90	公斤	280	25200
小计（元）		1465060				
<b>三、政务网络传输和各类视频会议运维</b>						
<b>1、政务网日常检修和运维</b>						
序号	项目	内容	单位	数量	单价(元)	总价(元)
1	自建光缆	线路检修维护	千米	70	800	56000
2	汇聚点	光纤ODF架检修维护	个	9	2000	18000
3	光纤熔接点	熔接点检修维护	点	1900	30	57000
4	核心交换机	硬件检查、监控、配置优化、故障排除、配件维修	套	4	5000	20000
5	汇聚交换机	硬件检查、监控、配置优化、故障排除、配件维修	台	35	800	28000
6	接入交换机	硬件检查、监控、配置优化、故障排除、设备维保（维修或更换）	台	240	400	96000
7	服务器	硬件检查、监控、配置优化、故障排除	台	20	1000	20000
8	路由器	硬件检查、监控、配置优化、故障排除	台	11	1000	11000

9	防火墙	硬件检查、监控、配置优化、故障排除	台	2	3000	6000
10	电源柜	硬件检查、监控、故障排除	套	2	3000	6000
11	机房空调	硬件检查、监控、故障排除	只	2	3000	6000
12	监控	硬件检查、监控、配置优化、故障排除	套	1	2000	2000
13	配电柜	硬件检查、监控、故障排除	套	2	2000	4000
14	UPS电源	硬件检查、监控、故障排除	套	5	1000	5000
15	电池组	硬件检查、监控、维护、充放电	块	56	200	11200
16	消防设施	硬件检查、监控、故障排除	套	1	2000	2000
17	设备间空调	硬件检查、监控、故障排除	台	14	600	8400
18	门禁	硬件检查、监控、故障排除	套	1	800	800
19	显示屏	硬件检查、监控、故障排除	套	2	800	1600
20	显示大屏	硬件检查、维护、配合展示	套	1	3000	3000
21	用户终端	根据用户需要解决网络及应用故障	台	3000	80	240000
22	病毒查杀	用户终端病毒查杀	台	3000	30	90000
23	光纤模块	单模20公里	个	100	180	18000
24	备品备件	交换机	台	20	2650	53000
25	标签机耗材	标签机、测线器及耗材	项	1	10800	10800

小计（元）

773800

## 2、视频专线检修及运维

序号	产品名称	产品规格	数量	单位	单价(元)	总价(元)
1	视频会议现场保障	技术人员4人、司机1人	12	月	30000	360000
2	车辆使用费	工具车	12	月	5000	60000
3	视频会议终端（备）	视频会议终端备用机	2	台	28500	57000
4	高清摄像机（备）	高清摄像机备用机	2	台	15200	30400
5	光纤模块	单模模块	12	个	150	1800
6	线路检修维护	技术人员2人	12	月	11000	132000
7	系统集成费		5	间	5000	25000

小计（元）

666200

## 四、电子政务网络光缆建设

序号	货品名称	规格型号	数量	单位	单价(元)	总价(元)
1	光缆	24芯	12000	米	4.4	52800
2	光缆	48芯	50000	米	6.2	310000
3	光缆	96芯	15000	米	11.9	178500
4	光缆交接箱	48芯	32	个	1850	59200
5	光缆交接箱	96芯	6	个	2850	17100
6	熔接点	中心机房	600	芯	20	12000
7	熔接点	汇聚点	1200	芯	20	24000
8	光纤终端盒	4进12出	20	个	150	3000
9	光纤终端盒	4进24出	20	个	180	3600
10	光纤终端盒	2进8出	10	个	50	500
11	法兰	DN80	1500	个	5	7500
12	尾纤	FC-1.5m-9/125	1500	条	8	12000
13	跳线	3米	1500	条	12	18000
14	挂钩	25#	1200	个	0.6	720
15	铁丝	8号	6000	米	5.3	31800
16	施工费	架空点到点进机柜	77000	米	2.8	215600
17	综合管理费	运输、保险、税费等	1	项	15000	15000
18	辅材		1	批	13280	13280
<b>小计(元)</b>		<b>974600</b>				
<b>服务期限</b>	本项目合同有效期：自合同签订之日起1年。本项目履行期限三年（一次招标三年沿用），实行一年一考核一签合同的办法，合同每年签订一次。一年期满后，采购人根据相关政策以及成交供应商服务质量与成交供应商续签下一年合同，以本次采购内容及报价为依据					
<b>投标总报价(元/年)</b>						
(大写)：壹仟叁佰柒拾捌万壹仟陆佰陆拾元整 (小写：¥13781660.00元/年)						

备注：1、本项目签订固定总价合同。投标报价应是完成招标内容所需的全部费用。投标人漏报或不报，招标人将视为有关费用已包括在投标报价中而不予支付，投标报价是投标人为完成本项目要求的全部服务内容最终价格的体现。

2、报价建议精确到小数点后2位。

3、各投标人根据招标文件的规定，结合企业自身管理水平及市场行情自主报价，投标人的投标报价大于等于上限控制价时，按无效投标处理。

投 标 人：延安高度科技有限责任公司（盖单位章）

法定代表人（单位负责人）或委托代理人：刘佳（签名）

日 期：2026年2月12日