**第五章 采购需求**

1.项目编号：11011825210200010184-XM001

2.项目名称：密云区电子政务外网IPv6升级改造项目

3.项目的七部分

|  |  |
| --- | --- |
| 序号 | 项目名称 |
| 一 | 出口链路 |
| （一） | 互联网IPv6出口链路 |
| （二） | 北京市电子政务外网出口链路 |
| 二 | 内网安全设备 |
| 三 | IPv6协议转换平台 |
| 四 | 域名及地址管理分配部分 |
| 五 | 集中办公区网络设备升级改造部分 |
| 六 | 集中办公区网络升级辅助施工部分 |
| 七 | 网络核心、集中办公区双栈调试费部分 |

4.采购需求：

**（一）采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求；**

为贯彻落实党中央、国务院关于建设网络强国和数字中国的战略部署，国务院办公厅于2017年印发《推进互联网协议第六版（IPv6）规模部署行动计划》，明确要求政务外网在 2025 年底前具备IPv6支撑能力，构建“高速、移动、安全、泛在” 的新一代信息基础设施。2023 年，工业和信息化部等八部门进一步发布《关于推进IPv6技术演进和应用创新发展的实施意见》，强调在政务网络中推广“IPv6+”技术（如分段路由、随流检测等），以提升网络安全隔离、快速开通恢复和故障定位能力，支撑政府治理水平全面提升。

本项目范围：

为了在2025年年底前完成政务外网具备IPv6支撑能力的目标，开展此项招标活动，本项目涉及的范围包括密云区电子政务外网核心区、区政府集中办公区、政务服务和数据管理局集中办公区的IPv6升级改造，其他各委办局、乡镇、行政村、企业等不在本项目范围内。

具体工作内容如下：

1. 替换老旧交换机，使网络平台支持双栈运行模式。
2. 替换老旧安全设备，保证双栈模式下的网络安全。
3. 增加具备双栈支撑能力的域名解析、地址管理与分配系统。
4. 保证现有业务系统在双栈模式下稳定运行。
5. 全网IPv6地址规划。
6. 双栈模式下网络拓扑设计。
7. 双栈模式下的集成服务。
8. 售后及培训等。

**（二）采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范；**

1. 中共中央办公厅、国务院办公厅印发的《推进互联网协议第六版（IPv6）规模部署行动计划》
2. 工业和信息化部等八部门进一步发布《关于推进 IPv6 技术演进和应用创新发展的实施意见》
3. 《北京市经济和信息化局关于加快推进区级政务外网IPv6升级改造工作的通知》（京经信发[2024]57号文）文件。
4. 《公共区域名系统（DNS）技术规范》GW0201-2024
5. 国家电子政务外网管理中心办公室印发的IPv6演进路线图和实施技术指南—政务外网
6. 国家电子政务外网管理中心办公室关于政务外网IPv6演进技术白皮书（2021）
7. 国家电子政务外网IPv6地址规划征求意见稿
8. GB/T22239-2019信息安全技术网络安全等级保护基本要求
9. GB/T25058-2019信息安全技术信息系统安全等级保护实施指南
10. GB/T 25070-2019信息安全技术网络安全等级保护安全设计技术要求
11. GB/T 20270-2006信息安全技术网络基础安全技术要求
12. **采购标的需求；**

1.需求详细表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | | **设备名称** | | | **参数** | **单位** | | **数量** | **备注** |
| **一、出口链路** | | | | | | | | | |
| **（一）、互联网IPv6出口链路** | | | | | | | | | |
| 1 | | 防火墙 | | | 2U标准机架式,内存≥32G，1个MGMT口，1个HA口,冗余电源,至少4个万兆光口，4个扩展槽位,防火墙吞吐量≥50G，并发连接≥1200万，每秒新建连接≥36万，应用层吞吐量≥40G，IPSEC VPN隧道数≥2000，SSL VPN吞吐≥2.5G，SSL VPN并发用户数≥5000 。包含应用识别功能，含1年应用特征库升级许可。防病毒库3年升级服务许可；三年硬件免费保修服务。 | 台 | | 1 |  |
| 2 | | 上网行为管理系统 | | | 2U标准机架式，至少6个千兆电接口，4个千兆光接口，4个万兆光口，1个扩展槽位。双电源，存储容量≥4T。网络层吞吐量≥27G，最大并发连接≥4000万，每秒新建连接≥40万，适用于6G带宽接入网络。提供三年免费特征库升级服务及三年硬件免费质保服务。 | 块 | | 1 |  |
| 3 | | 负载均衡 | | | 2U标准机架式,内存≥32G，至少标配6个千兆电口（含1个管理口，1个HA口）；4个千兆光口插槽；6个万兆光口插槽（含模块）,双电源,2个扩展槽位,负载均衡吞吐≥40G，并发连接≥2000万，四层新建≥60W，七层新建≥64W，三年硬件免费质保服务。 | 块 | | 1 |  |
| 4 | | 网络入侵防护系统 | | | 2U标准机架式,内存≥64G,至少2个千兆电口（含1个HA口和1个管理口），至少2个万兆SFP+插槽+光模块，支持Bypass，1个CONSOLE口,冗余电源,5个扩展槽位,整机吞吐率≥40Gbps，最大并发连接数≥2000万，IPS吞吐率≥20Gbps。3年攻击检测规则库、应用识别库、地理信息库升级许可； 1年僵尸主机规则库免费升级许可；三年硬件免费质保服务。 | 块 | | 1 |  |
| 5 | | 出口链路汇聚交换机 | | | 至少24个万兆SFP+，6个40/100GE QSFP28，包转发率≥1620Mpps，交换容量≥4.8/25.6Tbps，带4个万兆单模模块 | 台 | | 1 |  |
| **（二)、北京市电子政务外网出口链路** | | | | | | | | | |
| 1 | | 防火墙（含防病毒网关） | | | 2U机架式设备,内存≥16G。至少6个千兆电口，4个千兆光插槽,2个万兆光插槽。冗余电源,2个扩展槽位,防火墙吞吐≥20G，并发连接≥500万，每秒新建连接≥16万，应用层吞吐量≥16G，IPSEC VPN隧道数≥2000，SSL VPN吞吐量≥2.5G，SSL VPN并发用户数≥5000 。包含应用识别功能，含1年应用特征库升级许可。专业版快速扫描查杀病毒库3年免费升级服务许可；三年硬件免费质保服务。 | 台 | | 1 |  |
| 二、内网安全设备 | | | | | | | | | |
| 1 | | 堡垒机 | | | 2U机架式设备。至少6个千兆电口，4个千兆光口，1个Console管理口。存储容量≥8TB，双电源，带液晶面板，3个扩展槽。字符并发≥1500，图形并发≥400。被管资源数量无限制，至少包含200个被管资源数授权。提供三年硬件免费质保服务。 | 台 | | 1 |  |
| 2 | | 双因素认证 | 动态密码认证模块 | | CKEY动态认证系统支持多种终端令牌模式认证，适应于VPN/Citrix/VMWare View、Vcenter/堡垒机/KVM/云主机/交换机/业务系统/操作系统/安全设备等。实现网络资产用户在帐号+静态密码认证基础上多增加一层保护。整体提升安全防护、满足三级等保。内置认证服务、资源管理、策略管理、账号管理、日志审计、集成动态令牌认证引擎、生物识别认证引擎和RADIUS、TACACS+、LDAP协议服务。支持500资产规模。 | 套 | | 1 |  |
| 资产接入授权 | | 接入资产授权license：实现多个业务系统对接，例如OA、ERP、CRM等；多个网络设备对接，交换机、vpn、堡垒机、防护墙、网闸、IDS等；多个云主机、云桌面、操作系统等接入授权。（每接入一个资产IP会占用一个资产授权许可）含3年license许可。 | 授权 | | 100 |  |
| 软件令牌 | | 软件令牌形式，每隔60秒变化一个密码，支持Ios/android安装。包含3年license许可。 | 个 | | 5 |  |
| 用户账号许可 | | 员工账号用户授权许可。包含3年license许可。 | 个 | | 5 |  |
| 3 | | VPN | | | 标准2U机架式设备，1个RJ-45 Console口。至少8个10/100/1000M自适应电口，4个千兆SFP插槽，2个网络接口扩展槽位。2个USB口，交流冗余电源；整机吞吐率≥30Gbps，IPSec/SSL国密加解密吞吐率≥1Gbps，提供1000个SSL VPN并发用户授权，支持PC端和移动端同时接入。标配硬件加密卡，支持国家商用密码算法SM1、SM2、SM3、SM4，具备国家密码管理局发布的商用密码产品认证证书。提供三年产品硬件免费质保服务。 | 台 | | 1 |  |
| 4 | | 网络审计 | | | 标准2U机架式设备,内存≥32G，机械硬盘≥4T。至少2个千兆电口(1个管理，1个HA)，2个万兆光口含模块,冗余电源,2个扩展槽位。吞吐率≥8Gbps。包含数据库审计功能模块。包含应用识别功能，含1个云审计代理/Agent授权。三年硬件免费质保服务。 | 台 | | 1 |  |
| 5 | | 网络安全漏洞扫描系统 | | | 标准1U机架式设备。至少6个10/100/1000M Base-TX接口、4个千兆SFP接口，1个RJ45 Console口，2个USB接口，另具备2个接口扩展插槽，自带液晶屏，冗余电源。主机漏扫、配置核查、Web漏扫功能开通，主机漏扫和基线核查可扫描IP地址总数无限制，单任务最大可扫描≥300IP地址；主机漏扫并发扫描≥200IP地址；基线核查可核查Windows系列设备类型；Web漏扫可扫描子域名或IP总数量≥5个，Web漏扫并发≥5个子域名或IP。提供三年漏洞库免费升级服务及三年硬件免费质保服务。 | 块 | | 1 |  |
| 6 | | 态势感知平台流量探针 | | | 产品规格：标准2U机架式设备，冗余电源，1个RJ-45 Console口，1个10/100/1000 Base-Tx带外管理口。至少4个千兆电口，4个千兆光口，2万兆光口，6个扩展槽。硬盘≥8T，内存≥32G。 | 台 | | 1 |  |
| 产品功能：产品内置双向检测引擎、威胁情报引擎、AV检测引擎、yara检测引擎和机器学习检测引擎，搭载2W+检测规则，支持60+应用层协议解析，能对流量中的威胁进行检测、文件中的威胁进行检测；支持检测已知威胁、未知威胁；能对实时发生的网络威胁进行检测，也能基于通信特征对部署前已感染的网络威胁进行检测，覆盖威胁的全生命周期。 |
| 产品性能：实际网络处理能力≥6Gbps，最大并发连接≥700万，每秒新建连接数≥5万。 |
| 产品服务：三年免费威胁检测规则库、威胁情报库升级服务；三年产品免费保修服务升级服务，包含：硬件质保服务、技术支持服务、版本升级服务 |
| 7 | | 安全域接入交换机 | | | ≥24个万兆SFP+，≥6个40/100GE QSFP28，包转发率≥1620Mpps，交换容量≥4.8/25.6Tbps，4个万兆单模模块 | 台 | | 1 |  |
| 三、IPv6协议转换平台 | | | | | | | | | |
| 1 | | IPv6协议转换平台 | | | 一、服务器 配置参数 国产CPU≥16核,DDR4 3200 内存≥64G,存储≥2T；千兆端口：4个；设备吞吐率≥2 Gbps；最大并发连接数≥200万，最大新建连接数2万个/秒； 二、IPv6智能升级系统  三、IPv6WAF安全防护系统  四、IPv6防DDos攻击服务系统  五、三年免费运维服务  六、网站IPv6支持度检测服务 | 台 | | 1 |  |
| 四、域名及地址管理分配部分 | | | | | | | | | |
| 1 | | 统一管理节点 | | | 配置冗余交流电源，支持热插拔 | 台 | | 1 |  |
| 千兆电口≥10，支持扩展至（4口千兆光板卡\*1、2口万兆光板卡\*2），内存容量≥16G，硬盘≥2T，支持Raid1，可管理DNS和DHCP/IPAM服务节点，三年免费保修服务 |
| 2 | | DNS服务节点 | | | 配置冗余交流电源，支持热插拔 | 台 | | 1 |  |
| 千兆电口≥10，支持扩展至（4口千兆光板卡\*1、2口万兆光板卡\*2），内存容量≥16G，硬盘≥2T，支持Raid1，≥8万QPS，三年免费保修服务 |
| 3 | | DHCP/IPAM服务节点 | | | 配置冗余交流电源，支持热插拔 | 台 | | 1 |  |
| 千兆电口≥10，支持扩展至（4口千兆光板卡\*1、2口万兆光板卡\*2），内存容量≥16G，硬盘≥2T，支持Raid1，LPS≥500，DHCP 容量：≥8万，三年免费保修服务 |
| 五、集中办公区网络设备升级改造部分 | | | | | | | | | |
| 1、区政府集中办公区一号楼升级内容 | | | | | | | | | |
| 1.1 | | 汇聚交换机 | | | 交换容量≥102.4/403.2Tbps | 台 | | 1 |  |
| 包转发率≥57600MppS |
| 槽位数≥6 |
| 双电源\双主控\48千兆电口卡\*2，24千兆光口卡+24万光光口卡\*2 |
| 1.2 | | 接入交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 12 |  |
| 包转发率≥166Mpps |  |  |
| 交换容量≥672Gbps/6.72Tbps |
| 1.3 | | 服务器区交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 2 |  |
| 包转发率≥166Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 1.4 | | 服务器区交换机 | | | 24个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 1 |  |
| 包转发率≥126Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 1.5 | | 光模块 | | | 千兆单模10KM 1310 | 块 | | 30 |  |
| 2、区政府集中办公区二号楼升级内容 | | | | | | | | | |
| 2.1 | | 汇聚交换机 | | | 24个万兆SFP+，6个40/100GE QSFP28，包转发率≥1620Mpps，交换容量≥4.8/25.6Tbps，4个万兆单模模块 | 台 | | 1 |  |
| 2.2 | | 接入交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 6 |  |
| 包转发率≥166Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 2.3 | | 光模块 | | | 千兆单模10KM 1310 | 块 | | 12 |  |
| 3、区政府集中办公区三号楼升级内容 | | | | | | | | | |
| 3.1 | | 汇聚交换机 | | | 24个万兆SFP+，6个40/100GE QSFP28，包转发率≥1620Mpps，交换容量≥4.8/25.6Tbps，4个万兆单模模块 | 台 | | 1 |  |
| 3.2 | | 接入交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 13 |  |
| 包转发率≥166Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 3.3 | | 接入交换机 | | | 24个10/100/1000BASE-T以太网端口,4个万兆SFP+，包转发率≥126Mpps ，交换容量≥672Gbps/6.72Tbps | 台 | | 1 |  |
| 3.4 | | 服务器区交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 1 |  |
| 包转发率≥166Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 3.5 | | 服务器区交换机 | | | 24个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 7 |  |
| 包转发率≥126Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 3.6 | | 光模块 | | | 千兆单模10KM 1310 | 块 | | 44 |  |
| 4、政务服务和数据管理局集中办公区网络设备升级改造部分 | | | | | | | | | |
| 4.1 | | 汇聚交换机 | | | 24个万兆SFP+，6个40/100GE QSFP28，包转发率≥1620Mpps，交换容量≥4.8/25.6Tbps，4个万兆单模模块 | 台 | | 1 |  |
| 4.2 | | 交换机 | | | 48个10/100/1000BASE-T以太网端口,4个万兆SFP+ | 台 | | 11 |  |
| 包转发率≥166Mpps |
| 交换容量≥672Gbps/6.72Tbps |
| 4.3 | | 光模块 | | | 千兆单模10KM 1310 | 块 | | 22 |  |
| 4.5 | | 叫号系统硬件部分 | | | 为了适应新主板安装，需要对机箱背板做钣金定制 | 套 | | 40 |  |
| 包含主板（支持IPv6升级版），CPU：参数 主频≥2.7Ghz，核数≥2，线程数≥4，内存≥4G，固态硬盘≥256G | 套 | | 40 |  |
| 叫号系统软件开发 | | | 基于Windows系统做定制软件开发 1、 UI设计、2、叫号信息展示页面开发 3、队列竖屏展示页面开发 | 人套 | | 44 |  |
| 1.设备绑定及相关接口软件开发 2. 队列推送及相关接口软件开发 3.叫号推送及相关接口软件开发 | 人套 | | 40 |  |
| **六、集中办公区网络升级辅助施工部分**  **（详见《密云区电子政务外网IPv6升级改造项目-集中办公区网络升级辅助施工部分-工程量清单》）** | | | | | | | | | |
| **七、网络核心、集中办公区双栈调试** | | | | | | | | | |
| **序号** | **服务项目** | | | **工作内容** | | | **人/天** | | |
| 1 | IPv6地址规划 | | | 详细描述全网的IPv6地址规划方案，具体到设备管理IPv6地址规划、网间路由地址规划、按业务地址规划、按部门地址规划，部门规划到村级。指明应答文件所在章节页号。 | | | 95 | | |
| 2 | 网络核心双栈配置改造（10508\*2台） | | | 依据核心交换机的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 40 | | |
| 3 | 3号楼汇聚交换机（10504\*1台） | | | 依据该设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 20 | | |
| 4 | 出口链路双栈配置改造（10台） | | | 依据各个设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 100 | | |
| 5 | 移动接入平台双栈配置改造（3台） | | | 依据各个设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 60 | | |
| 6 | 北京市政务网防火墙双栈配置改造 | | | 依据该个设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 20 | | |
| 7 | 集中办公区双栈配置改造（60台） | | | 依据各个设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 60 | | |
| 8 | 委办局汇聚双栈配置改造 | | | 依据该设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 20 | | |
| 9 | 镇街汇聚双栈配置改造（9306） | | | 依据该设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 20 | | |
| 10 | 村村通汇聚双栈配置改造（9306） | | | 依据该设备的功能，做出相应的配置策略及内容。指明应答文件所在章节页号。 | | | 20 | | |
| 11 | 全网性能优化（1项） | | | 详细描述全网性能优化的的内容及预期效果。指明应答文件所在章节页号。 | | | 100 | | |
| 12 | PC机IPv6升级 | | | 详细描述全网性能优化的的内容及预期效果。指明应答文件所在章节页号。 | | | 65 | | |

**注：每个项目的集成费由各投标单位自行报价，并计入本项目各项报价总和。**

2、第六部分需求

2-1、工程概况

工程名称：密云区电子政务外网IPv6升级改造项目-集中办公区网络升级辅助施工部分

工程地址：北京市密云区鼓楼西大街3号

建设单位：北京市密云区数据中心（本级）

2-2、编制范围

1号楼辅助施工部分：老旧设备拆除、老旧防雷组件拆除、数据跳线安装、

线缆整理。

2号楼辅助施工部分：老旧设备拆除，壁挂机柜、电源电缆、配线架、理线

架、数据跳线安装，线缆整理，室内光缆铺设等。

3号楼辅助施工部分：老旧设备拆除，壁挂机柜、数据跳线安装，线缆整理

室内光缆铺设等。

政务服务和数据管理局集中办公区网络设备升级改造辅助施工部分：老旧

设备拆除、数据跳线安装、线缆整理。

2-3、编制依据

建设单位要求。

与项目相关的国家及地方规范、技术标准。

北京市建设工程工程量清单计算标准(2021-北京)、北京市房屋修缮工程量清

单计算标准(2023-北京) 及配套计量规范。

2-4、费用说明：

招标控制价合计： 135541.96 元；

其中：

分部分项工程合价为： 121389.91 元；

措施项目： 2960.51 元；

其他项目合价为： / 元；

税金合价为： 11191.54 元；

其他说明：

规费(不含税)合计金额： 5056.81 元；

专业工程暂估价（含税）合计金额： / 元；

材料和工程设备暂估价（含税）合计金额： / 元；

暂列金（不含计日工）（含税）合计金额： / 元；

安全文明施工费（含税）合计金额： 3001.1 元；

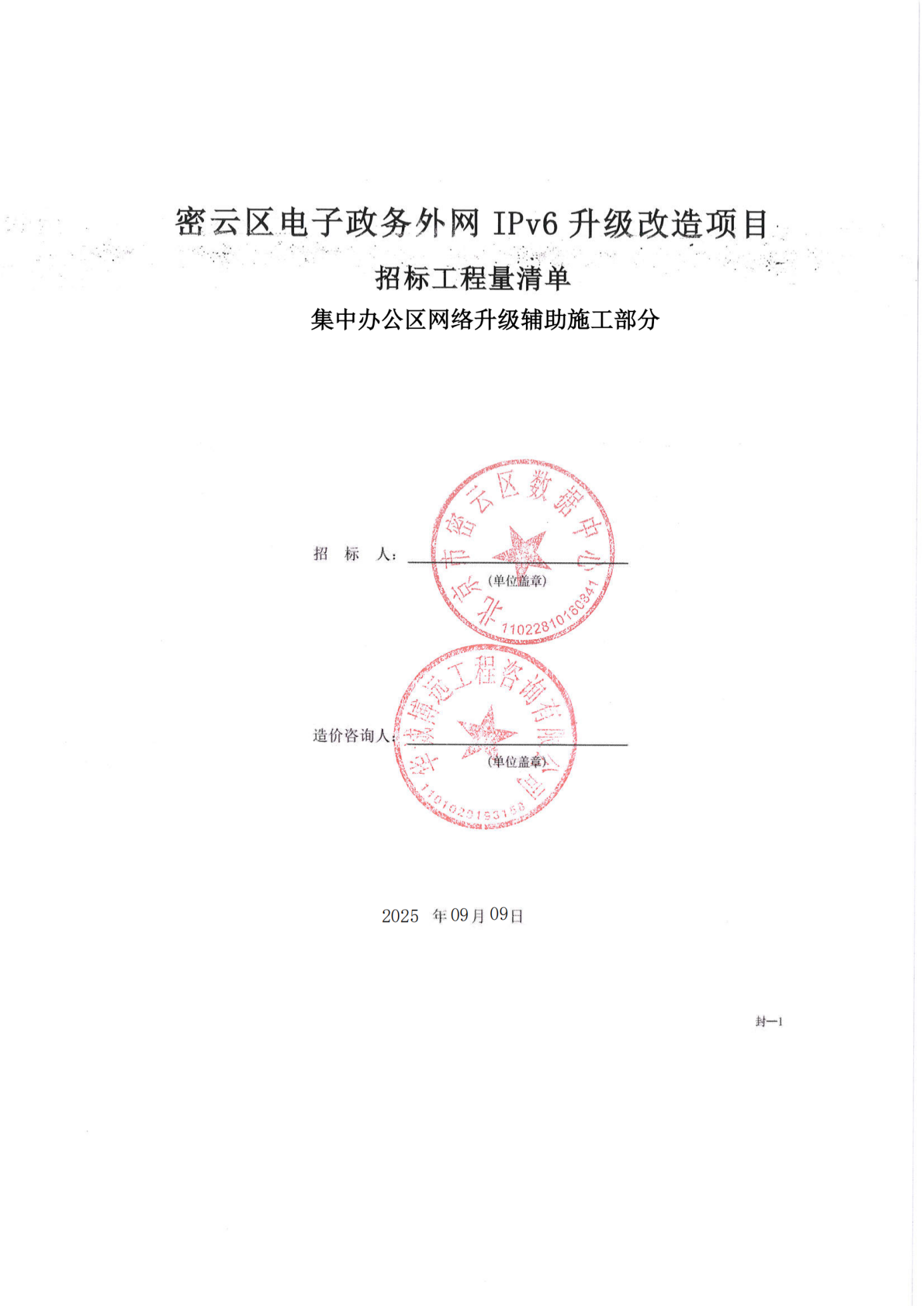
赶工费增加（含税）合计金额（如有）： / 元。

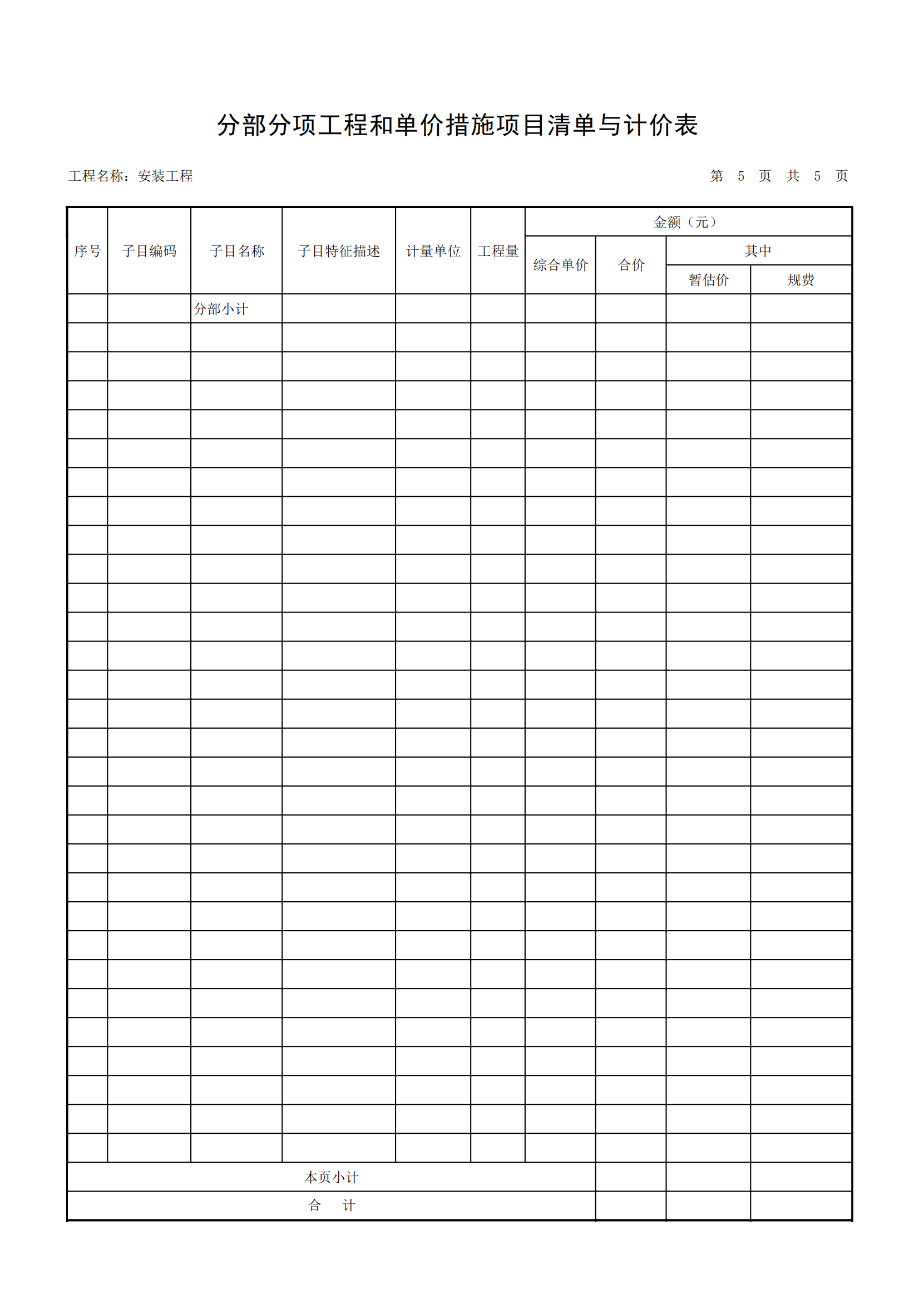
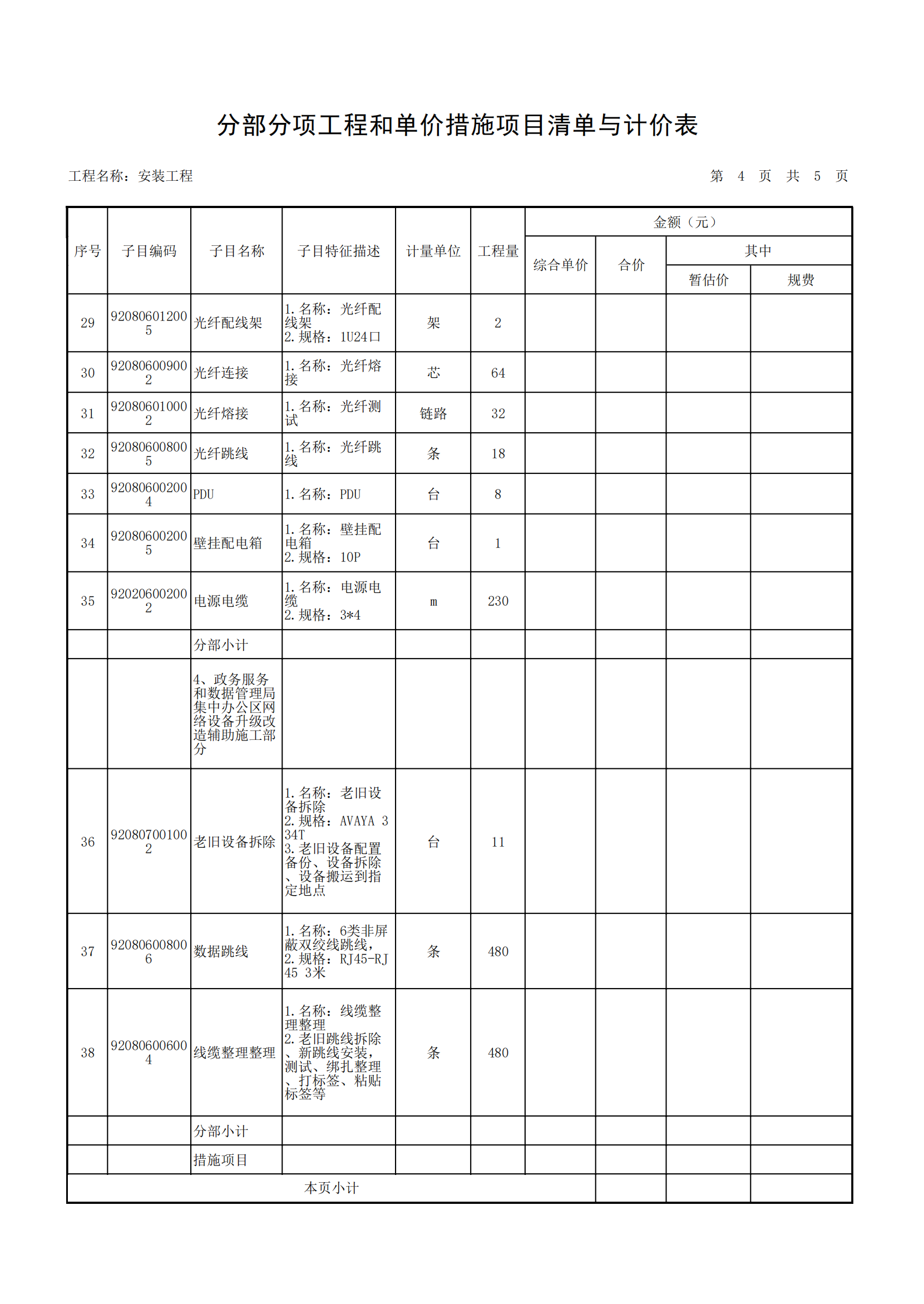
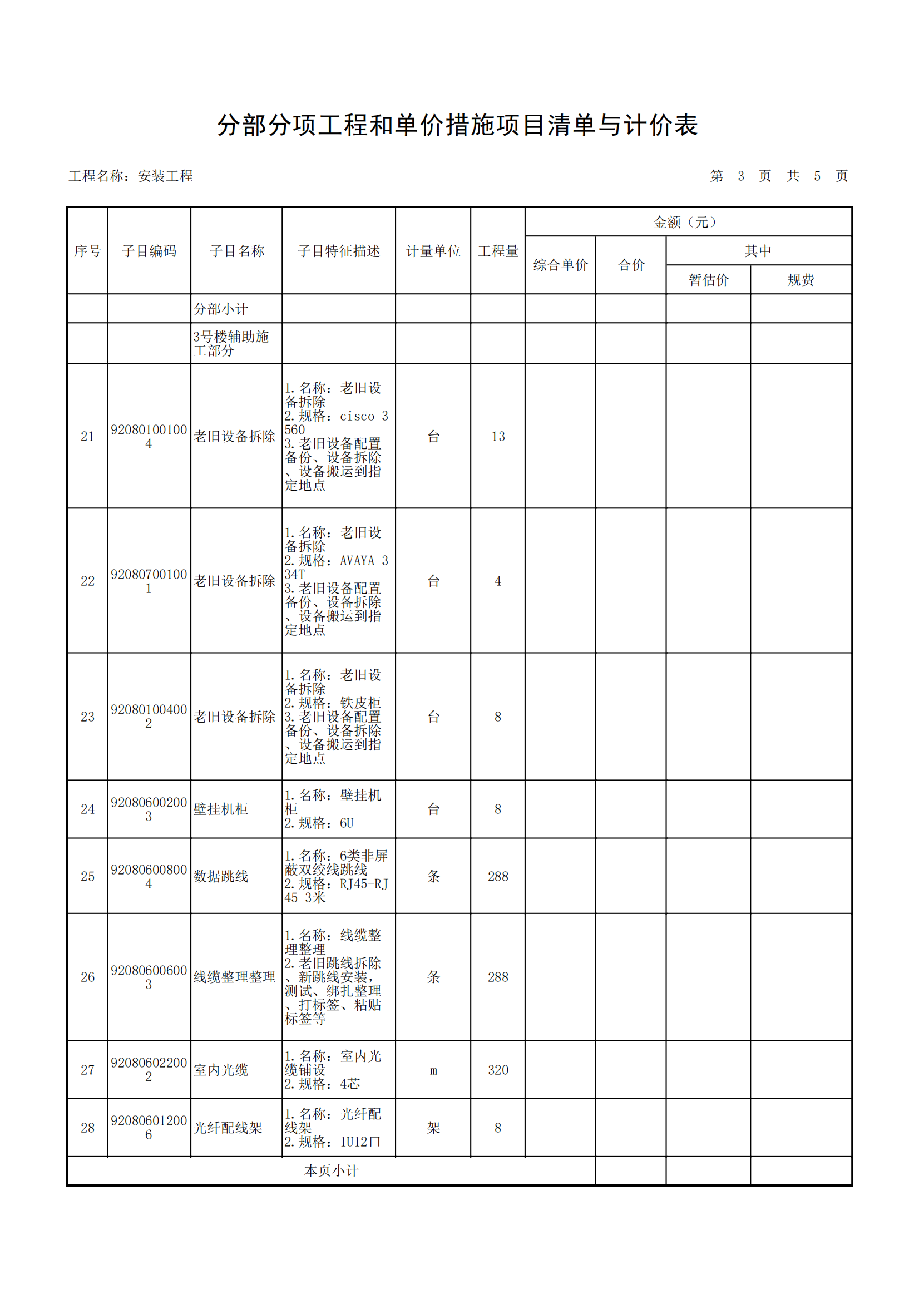
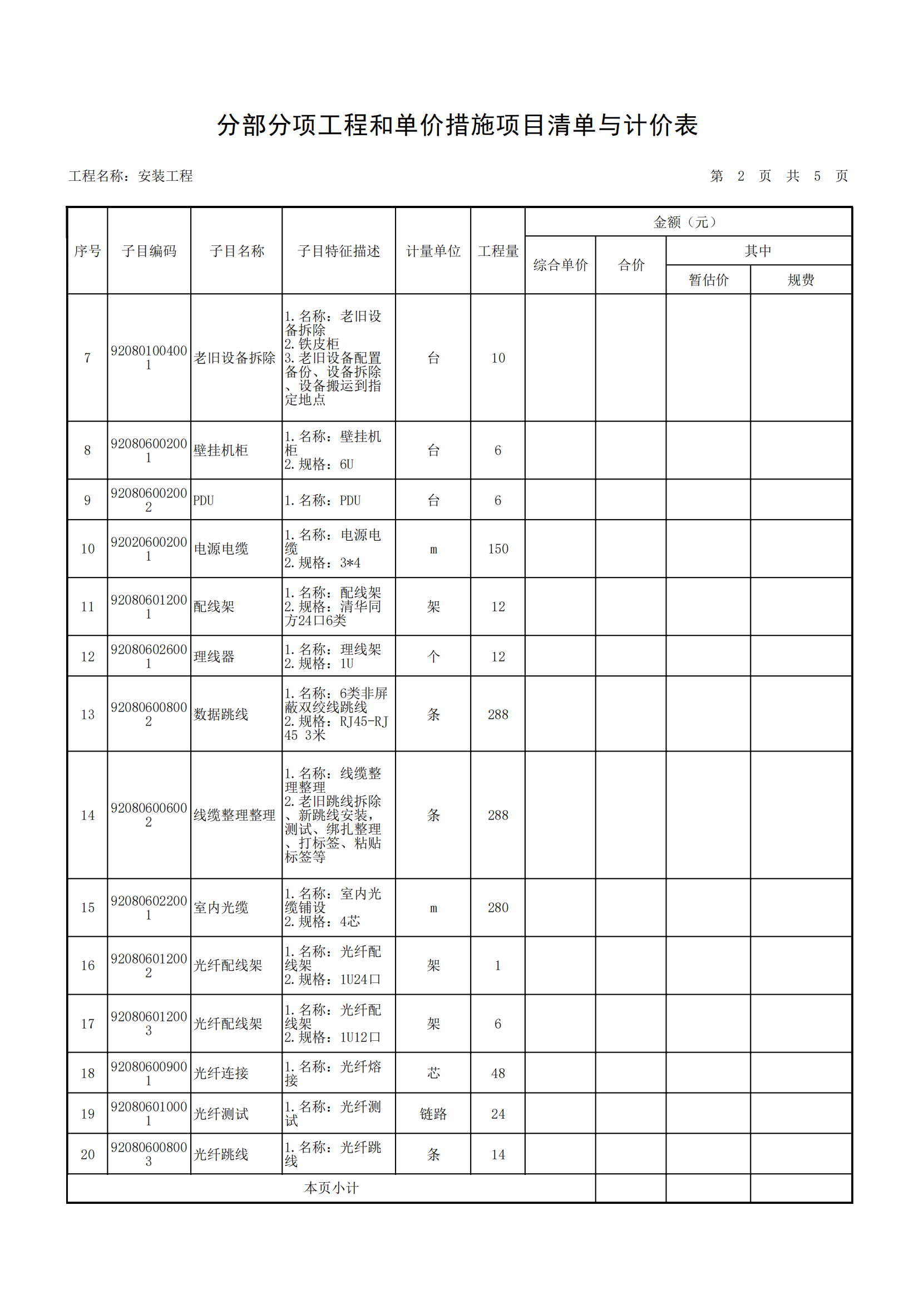
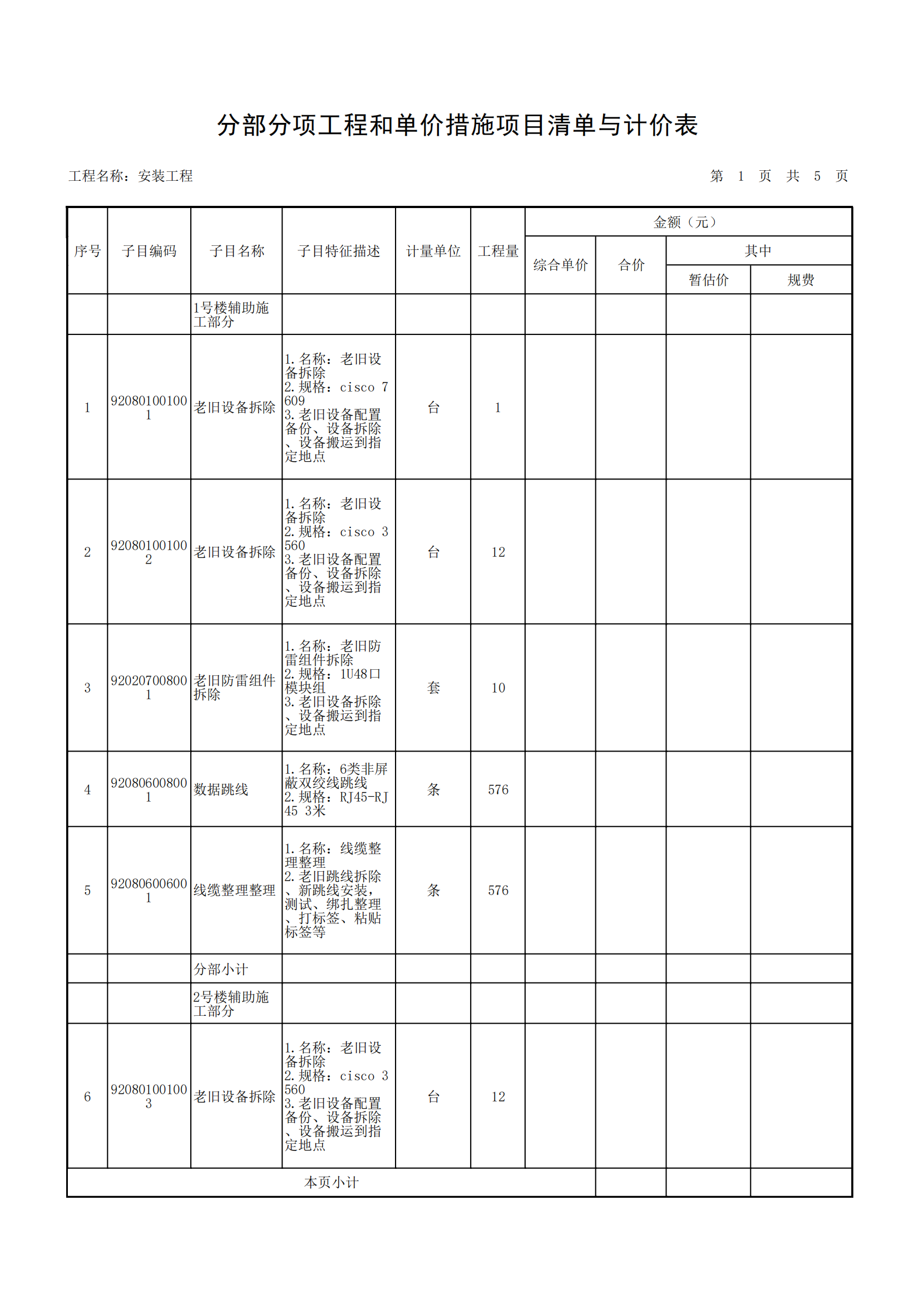
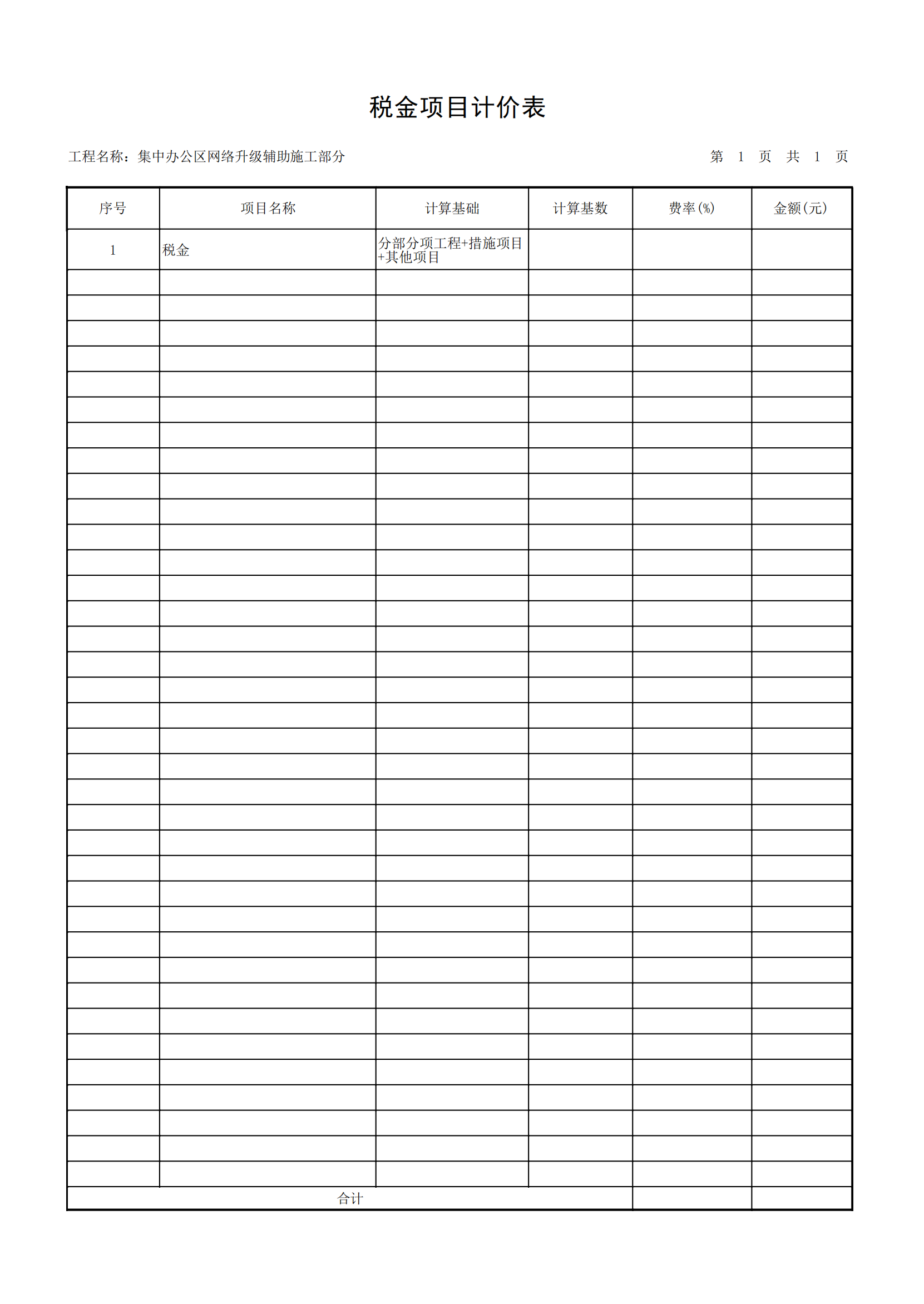
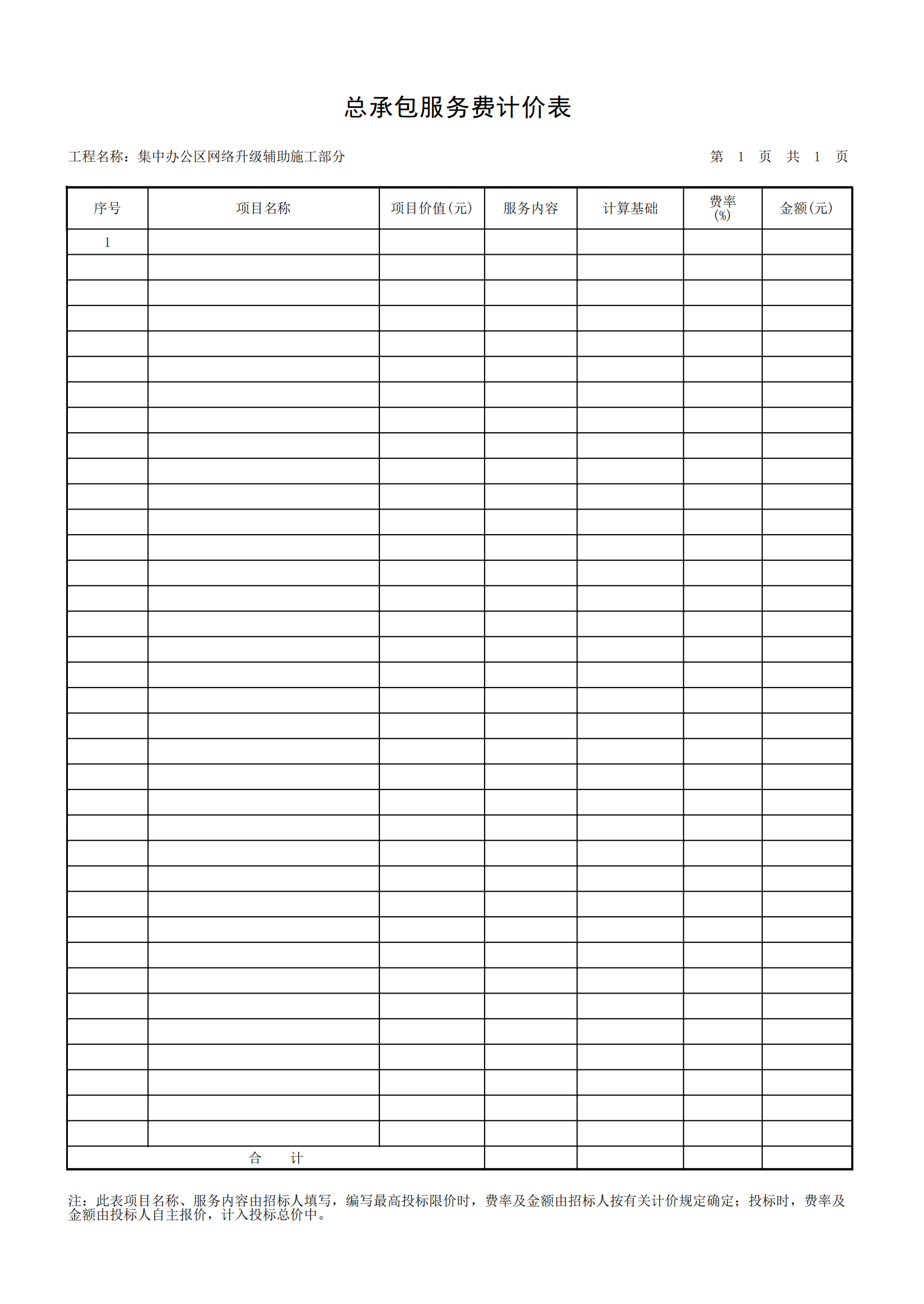
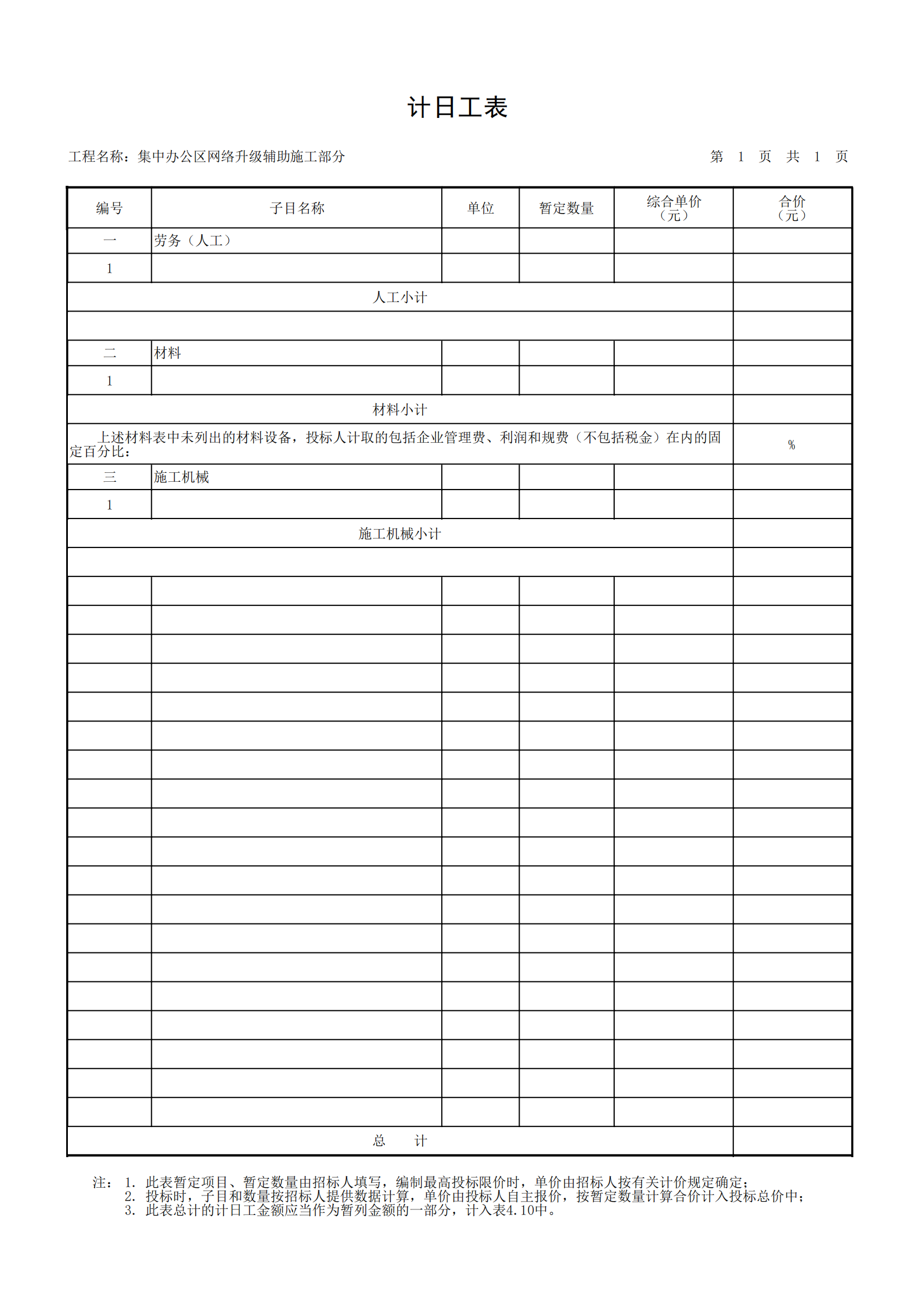
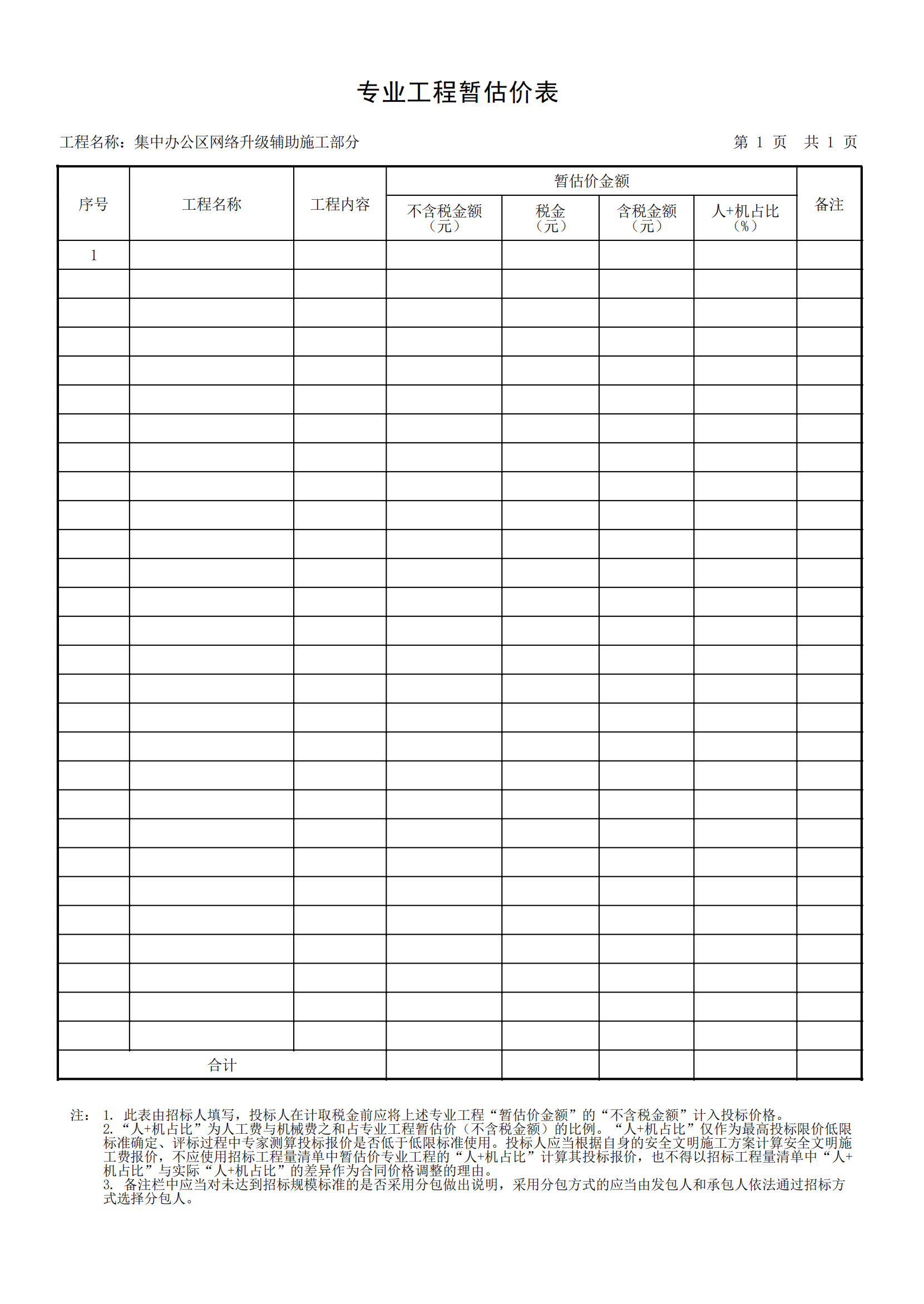
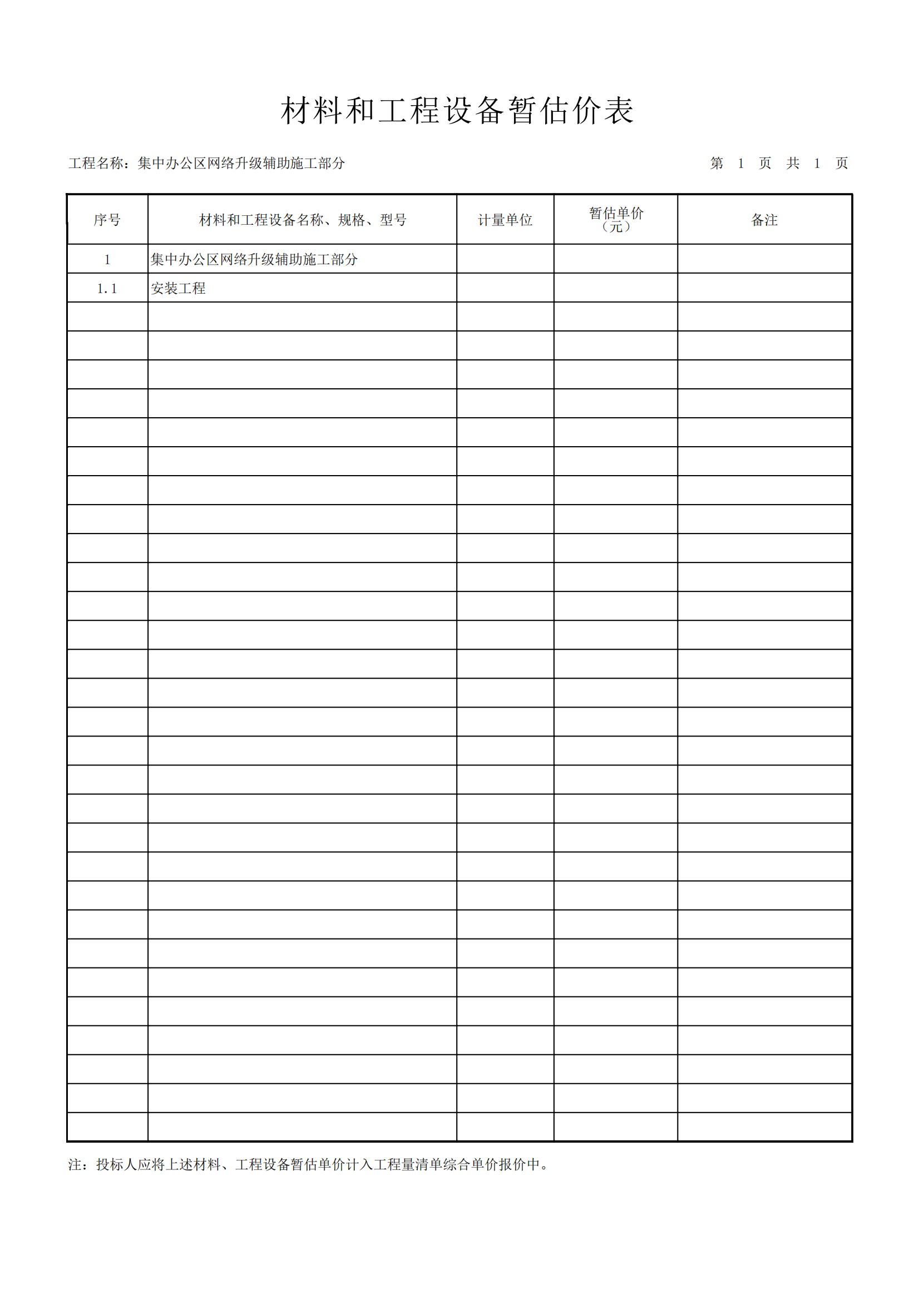
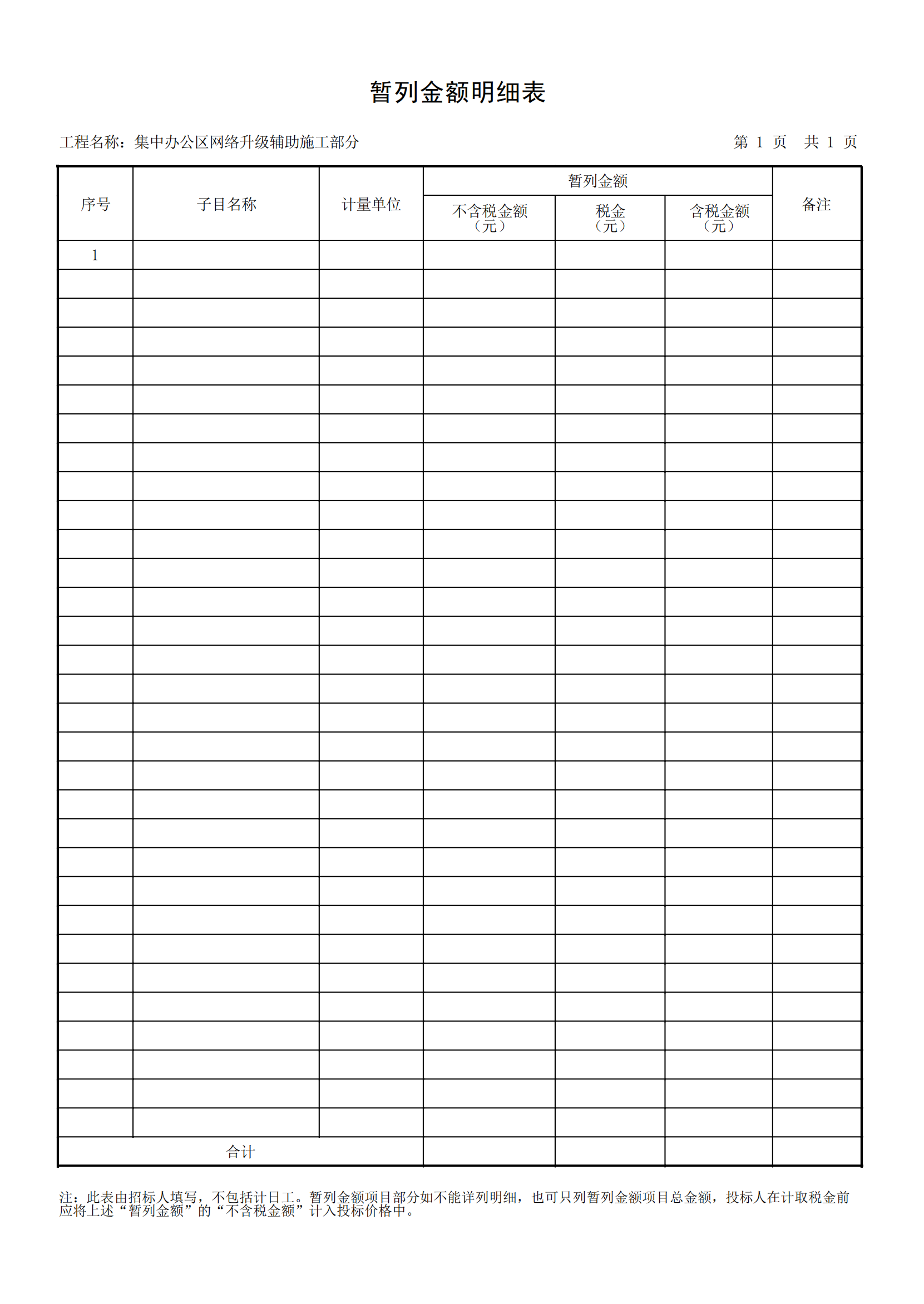
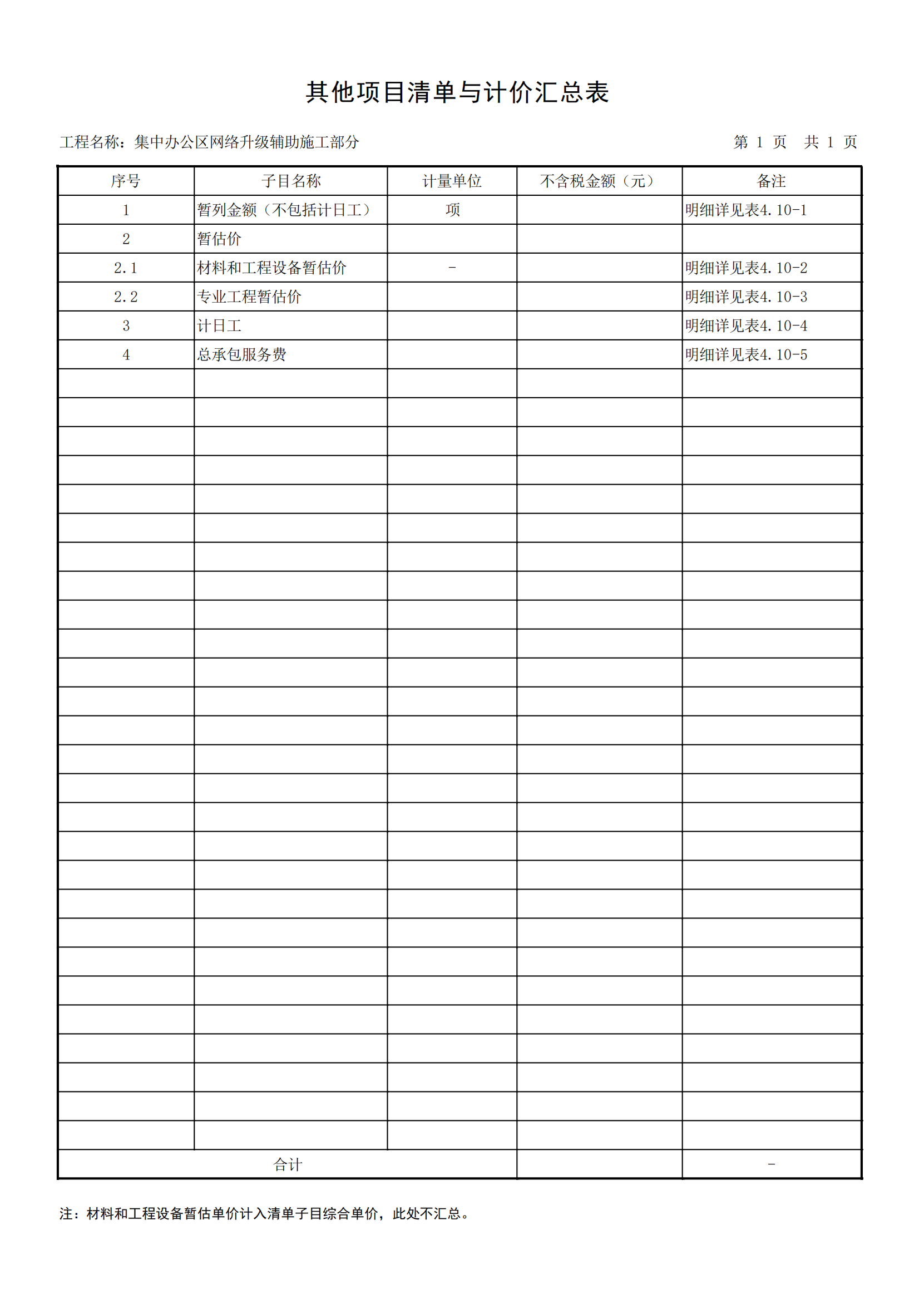
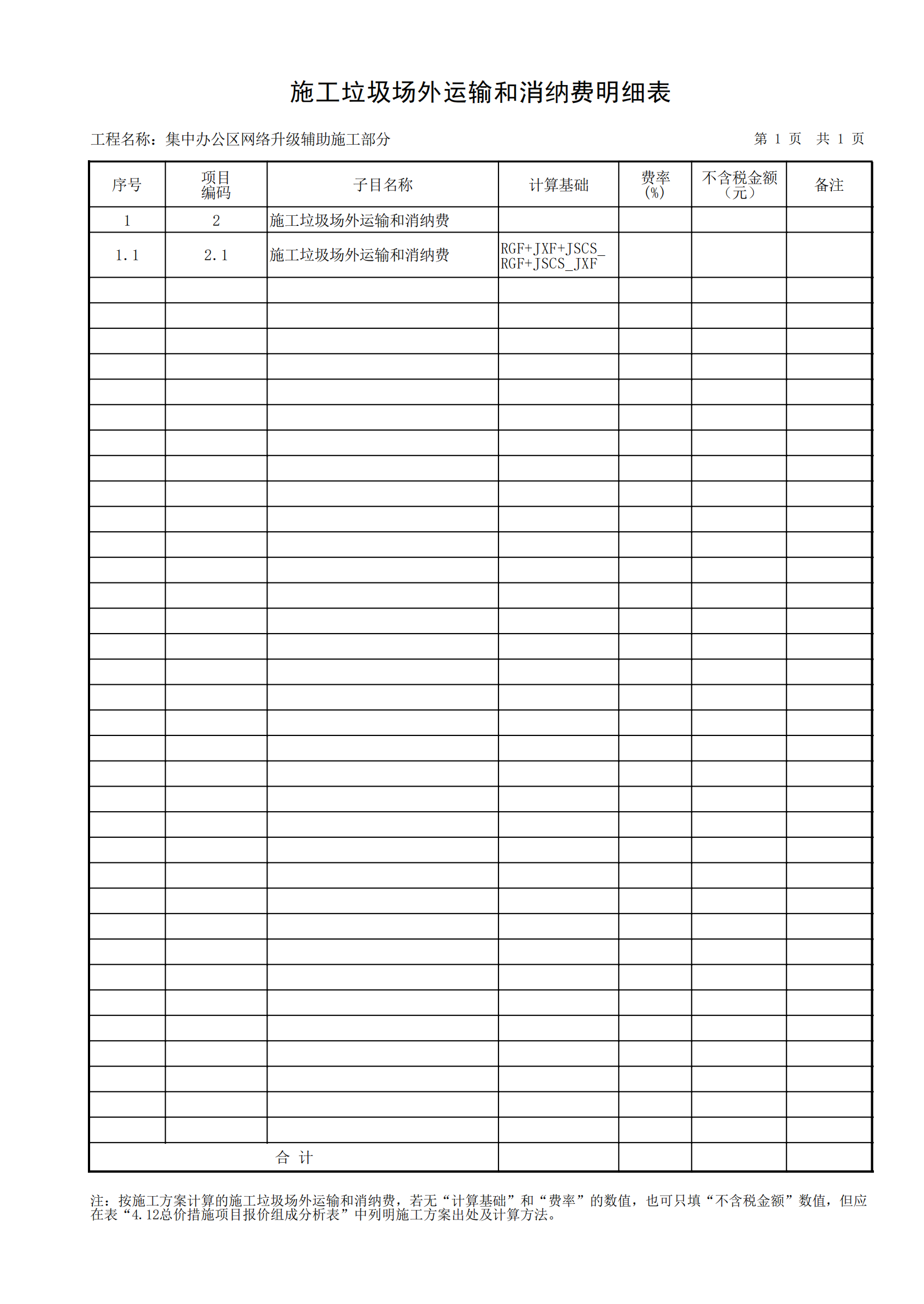
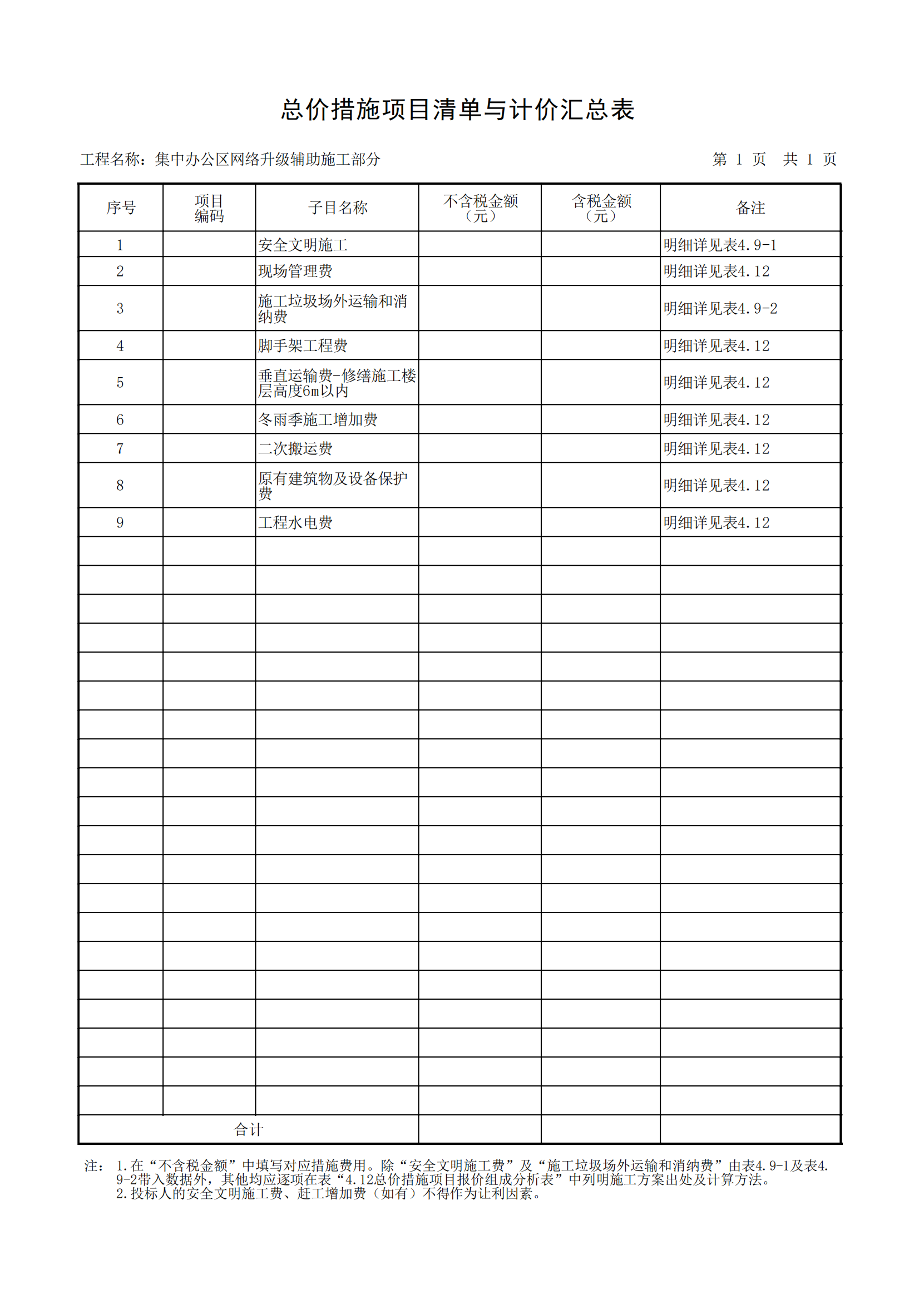
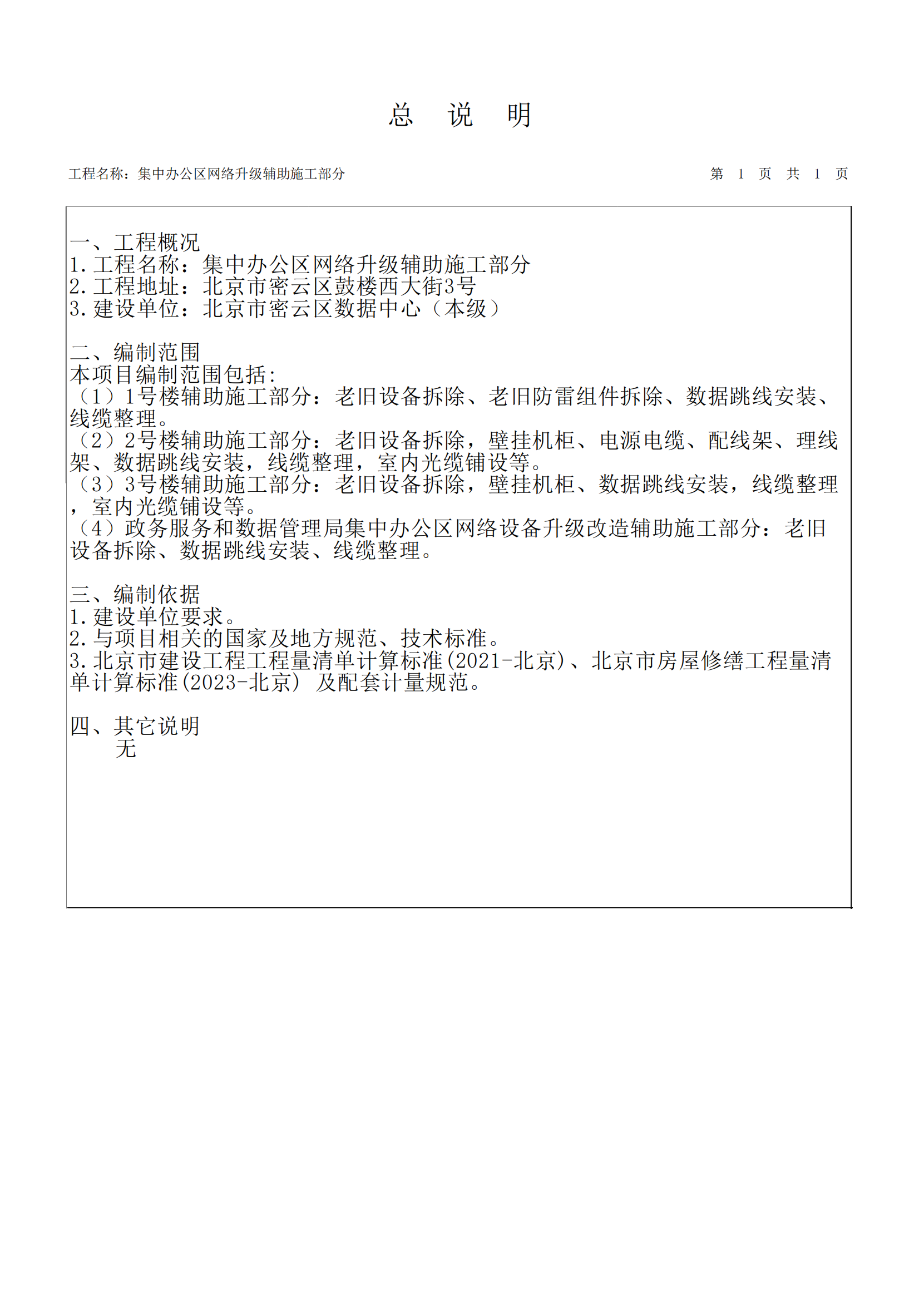
2-5、其它说明：工程量清单需要加盖造价工程师专用章、单位公章、法人或授权人签字或盖章。

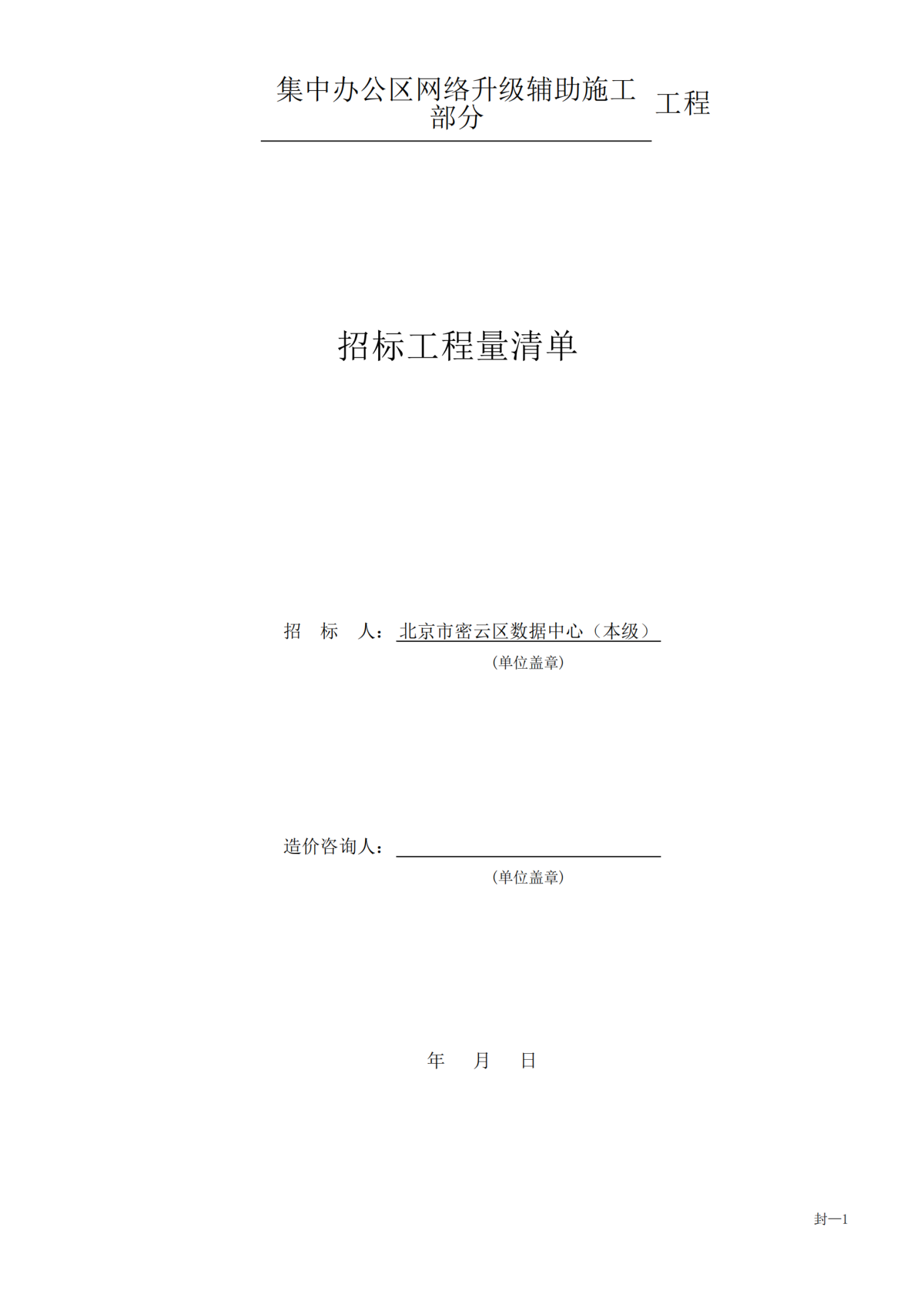
**2-6、项目实施概况**

|  |  |  |
| --- | --- | --- |
| **序号** | **单位名称** | **要求完成时间** |
| 1 | 密云区政府集中办公区 | 自签定合同之日起90天内完成 |
| 2 | 密云区政务服务和数据管理局 | 自签定合同之日起90天内完成 |

2-7、**《密云区电子政务外网IPv6升级改造项目-集中办公区网络升级辅助施工部分-工程量清单》**

****

****



**（四）、产品功能要求（1-4部分）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **功能要求** | | | **备注** |
| **一、出口链路** | | | | | |
| **（一）、互联网出口链路** | | | | | |
| 1 | 互联网出口防火墙 | 路由交换 | | ▲支持RIP、OSPF、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM；支持策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP/MAC绑定 | | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 地址转换 | | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 链路负载均衡 | | 支持链路负载均衡功能，支持轮询、加权轮询、就近选路、优先级、带宽比率等多种链路负载均衡算法，支持备用选路算法，支持链路过载保护。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DNS 双向智能转换 | | 防火墙作为 DNS 服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 访问控制 | | 支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、数据库防护、防代理、APT等功能配置,简化用户管理；访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行Web认证，策略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略；提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析、宽泛策略分析，可在WEB界面显示检测结果。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 网络接入 | | 支持RADVD、ND、RIPng、OSPFv3、BGP4+，支持IPv6静态、动态组播路由；支持NAT64、NAT46、NAT66地址转换，支持6to4隧道、ISATAP隧道。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IPv6访问控制 | | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DDOS 防御 | | 支持 HTTP DDOS 防护，采用阀值检查、源/目的限流、源认证、会话限制等方式综合进行 HTTP FLOOD、HTTP URI CC 攻击、HTTP 连接耗尽等攻击防护；支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP QUERY FLOOD、NTPREPLY FLOOD 攻击防护。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资源虚拟化 | | 支持在一台物理设备上划分出128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于24个虚拟防火墙授权。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 功能虚拟化 | | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、僵木蠕、高级威胁防护、内容过滤、邮件安全、审计、报表、防代理等安全功能虚拟化。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资产管理 | | 支持管理员手动添加、批量导入、设备主动扫描、EDR资产上报、漏扫资产上报等多种资产信息获取方式，支持基于访问流量自动识别发现资产；支持对被控制端为内网资产的telnet、ssh、rdp等常用的远程控制协议进行跟踪，支持对内网资产提供socks5代理的情况进行跟踪。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 系统诊断 | | 支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP、HTTP、DNS诊断方式。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 审计 | | 支持独立审计策略，支持审计白名单；支持访问网站URL 地址、网页标题和网页内容审计；提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、FTP；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端IP、用户名、协议、上行流量、下行流量、总流量、时间等；支持基于应用、网站类型、用户对用户上网行为进行统计和排序；支持进行违规应用分析、违规网站分析、用户违规访问公示。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 日志 | | 支持日志外发至多个SYSLOG服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；日志存储模式支持空间模式和时间模式，时间模式下日志能够保存180天。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 联动功能 | | 支持与漏扫、EDR、DLP、WAF、防病毒网关、数据库审计设备联动，并提供有关部门的相关证书或测试报告。 | 出具相关证书或报告，**加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | 产品需具备信息安全产品自主原创证明。 | 出具相关证明，**加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ★产品需具备网络关键设备和网络安全专用产品安全认证证书、网络安全专用产品安全检测证书。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 2 | 上网行为管理系统 | 技术要求 | | 1.支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备。 |  |
| ▲2.内置应用识别规则库，应用规则数≥33500条，支持应用≥15000种，支持海外应用≥8500种的，移动应用≥2000种，URL库≥4000万，规则库应保证两周一更新。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 3.支持针对防盗链、CSRF攻击、CC等攻击行为进行防护；支持端口扫描功能；支持弱密码扫描功能，内置弱口令库，支持自定义字典库。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 4.支持全网威胁情报的搜索查询，可供攻击溯源，预知风险；支持不少于20种威胁分类，包括C&C、僵木蠕、勒索、钓鱼、垃圾邮件等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 5.支持策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，可在WEB界面显示检测结果；支持实时和周期性对所有安全策略进行分析。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 6.支持对HTTP、FTP、POP3、SMTP、IMAP协议的病毒进行查杀；支持多种压缩文件的病毒查杀。压缩默认支持5层，最大20层；支持查杀邮件正文/附件、网页及下载文件中包含的病毒。 |  |
| 7.内网资产监控，可对终端风险级别、操作系统、浏览器类型、应用、杀毒软件等方面进行监控。 |  |
| 8.支持健康检测，支持在某一时间段内逐级深入，并纂取任一时间内的详细信息，并可导出系统日志。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 9.支持威胁防御功能，支持基于源、目的、规则集的入侵检测；支持针对WEB服务器防护，包括网页防爬虫、网页防篡改、DDOS攻击防护、WEB攻击过滤等。 |  |
| 10.支持120+种翻墙代理软件的审计控制，可独立展示翻墙行为代理服务器所属地域、用户、用户组、应用等排行。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ★11.产品需符合《信息安全技术网络安全专用产品安全技术要求》和终端接入控制产品相关标准规范要求。（提供证书复印件，**加盖制造商公章**） | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 3 | 负载均衡 | 双栈接入 | | ▲支持IPV6/IPV4双栈，支持NAT66、NAT64、NAT46、DNS64可对过渡型网络进行负载均衡。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 链路入站负载均衡算法 | | 支持轮询算法、比率算法、拓扑算法、备用地址算法、丢包算法、最小连接数算法、最小往返延时算法、最小连接速率算法、最小跳数算法、最小包速率算法、最大带宽利用率算法。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 链路出站负载均衡算法 | | 支持轮询算法、比率算法、带宽比率算法、首个有效算法、随机算法、加权随机算法、丢包算法、最小连接数算法、加权最小连接数算法、最小流量算法、加权最小流量算法、观察者算法、最小包速率算法、最小带宽算法、最小连接速率算法、静态就近算法、动态就近算法、静态就近（HA）算法、源地址算法、目的地址算法、源地址和源端口算法。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DNS Server | | 支持主域名服务器、从域名服务器和转发域名服务器。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 地址库 | | 地址库包含国内ISP地址库、全国地址库和全球地址库，支持地址库手动导入，支持地址库查询。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 域名库 | | 域名地址库，内置国外域名地址库，可将访问国外域名的请求分发至指定线路，实现对国外域名访问的优化，支持自定义域名信息。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 服务器健康检查 | | 支持主动健康检查和被动健康检查相结合的方式；健康检查类型包括ICMP、TCP、TCP\_ECV、UDP、TCP被动、HTTP、HTTPS、FIX、SSL、SOAP、HTTP被动、RADIUS、LDAP、WAP、DNS、IMAP、POP3、SMTP、FTP、EXTERNAL、数据库等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| X-forward-for | | 支持X-forward-for，将客户端IP添加地址到 HTTP 请求报文的X-forward-for扩展头中，便于后期溯源。 |  |
| 数据库读写分离 | | 利用读写分离技术实现数据库负载且无需在服务器上安装任何插件或软件。通过对数据库操作请求做内容解析，将其中的写操作调度到指定服务器，减少服务器压力，提高数据库资源利用率，提升业务响应速度。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| SSL 卸载 | | 内置SSL 卸载模块，SSL工作减轻服务器负担。支持服务器CA证书导入，提供证书单向和双向认证，双向认证支持透传客户端证书给后台服务器。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 页面加速 | | 支持CSS加速功能，支持内嵌CSS,合并CSS,最小化CSS；支持JavaScript加速功能，支持内嵌JS，合并JS，最小化JS；支持HTML加速功能，支持去除空白，去除注释；支持图片加速功能，支持内嵌图片，转换图片格式。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 安全防护 | | 支持网络防火墙功能，支持基于源地址、源区域、源端口、目的地址、目的区域、服务、时间进行访问控制；支持Web应用防火墙功能，支持跨站脚本攻击(XSS)、扫描器防护(Scanner)、SQL注入攻击(SQLi)、系统命令注入攻击(OSI)、远程文件包含攻击(RFI)、路径遍历(Path Traversal)、信息泄露攻击(Info Leak)、LDAP 注入攻击(LDAPInjection)、XPath 注入攻击(XPathInjection)、SSI 注入攻击(SSI Injection)、Web 服务器漏洞攻击、Webshell 检测；支持数据库安全功能，检查访问数据库的权限，杜绝非授权用户访问数据，保证数据库的安全。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DDoS 防护 | | 支持四到七层抗DDoS攻击功能。支持IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、NTP、SIP。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 漏洞扫描 | | 提供漏洞扫描功能。设备内置漏洞特征库，可针对应用服务器或者整个IP网段进行定向扫描分析，发现服务器操作系统漏洞并生成漏洞分析报告。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| HTTP2.0 | | 支持HTTP2网关部署，在不改变web服务器的情况下将对外服务协议从HTTP1.1/1.0升级至HTTP/2，提升终端用户使用体验和业务安全性。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 系统管理 | | 支持标准的 RESTful 等形式的 API 接口，可与主流的自动化运维工具对接。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| VPN 功能 | | 支持 SSL VPN 功能。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | ▲产品需提供《IPv6 Ready Logo认证》证书。 | **（提供证书复印件，加盖制造商公章）** |
| 产品资质 | | ★产品需提供相关部门颁发的《网络安全专用产品安全检测证书》 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 4 | 网络入侵防护系统 | 受害者视角分析 | | 支持受害者视角分析，按照时间范围、受害主机、事件类型、处置状态、攻击结果、应用协议等条件综合分析受害者信息。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DDoS 分析 | | 支持DDoS 攻击事件分析，按照时间范围综合分析DDoS攻击类型分布、被攻击IP Top10、被攻击IP排名、被攻击IP流量排名等信息。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 流量分析 | | 支持流量视角分析，支持按照应用、接口、连接进行流量统计分析。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 攻击检测 | | 支持独立的攻击检测引擎，涵盖10000种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度、ATT&CK、攻击阶段等方式进行分类；支持对攻击逃逸报文进行深度智能检测，包括：IP分片、TCP分段、RPC分片分段、SMB分片分段、HTTP-Header折叠、HTTP-Body UTF-7编码、HTTP-Body UTF-16（LE/BE）编码、HTTP-Body UTF-32（LE/BE）编码、HTTP-Body压缩、HTTP-Post数据编码、邮件体编码、URL多重编码、URL斜线分隔符、URI相对目录欺骗、HTTP-Javascript编码、邮件头折叠等类型。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ARP攻击检测 | | 支持ARP攻击检测，支持基于ARP请求的源IP不合法、响应的源IP不合法、响应的目的 IP不合法、请求的源MAC与以太网源MAC不同、响应的源MAC与以太网源MAC不同、响应的目的MAC与以太网目的MAC不同进行检测。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 僵尸主机检测 | | 支持独立的僵尸主机检测引擎，涵盖11000种以上的僵尸主机规则库。规则库支持按照攻击类型、操作系统、风险等级、ATT&CK、攻击阶段等方式进行分类；支持能够检测包括：僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT等多类型的僵尸主机行为。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 异常流量检测 | | 支持DGA恶意域名检测，采用DGA恶意域名检测智慧引擎检测；支持HTTP隧道检测，采用HTTP隧道智慧引擎检测。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DDoS检测 | | 支持独立的DDoS检测引擎，支持对IP扫描攻击、端口扫描攻击等多种扫描攻击行为检测；支持IP FLOOD 攻击检测、IP FRAG FLOOD 攻击检测、DOS 攻击检测、ICMPFLOOD 攻击检测、TCP FLOOD 攻击检测、SYN FLOOD 攻击检测、ACK FLOOD 攻击检测、SYNACK FLOOD 攻击检测、FIN FLOOD 攻击检测、RST FLOOD 攻击检测、TCPFRAG FLOOD 攻击检测、UDP FLOOD 攻击检测、UDPFRAG FLOOD 攻击检测、DNS REQUEST FLOOD 攻击检测、DNS REPLY FLOOD 攻击检测、DNS 格式检查、HTTPFLOOD 攻击检测、HTTP 新建连接 FLOOD 攻击检测、HTTP 并发连接 FLOOD 攻击检测、HTTP URI CC 攻击检测、HTTP 自定义端口、HTTPS FLOOD 攻击检测、HTTPS 新建连接 FLOOD 攻击检测、HTTPS 并发连接FLOOD 攻击检测、HTTPS 自定义端口等多种 FLOOD 攻击检测。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持DDoS自学习模式检测，可设定学习时长，根据周期内流量状态自动学习，设置检测流量阈值，流量异常触发阈值系统自动进行告警。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| WEB防护 | | 支持注入和WEBSHELL攻击检测，包括：SQL语法分析引擎检测、SQL注入智慧引擎检测、XSS攻击智慧引擎检测、命令注入智慧引擎检测、WEBSHELL上传智慧引擎检测、WEBSHELL行为检测；支持爬虫检测，涵盖超过1900种爬虫类型。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 规则库升级 | | 支持规则库升级无缝加载技术，整个升级过程检测引擎工作不间断。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 加密流量检测 | | 支持卸载SSL，实现对HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MQTT、SIP等加密流量的分析检测；支持恶意加密流量检测，采用恶意TLS流量智慧引擎、异常握手、非法证书和内网流量检测恶意加密流量。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 多维联动 | | 支持与本次项目采购防火墙联动处置，发现威胁事件联动防火墙阻断。 |  |
| 自定义检测 | | 支持自定义检测，能够按照特征（五元组、应用协议、域名、URL、文件哈希、邮箱地址、证书、特征串、正则等）、Snort规则、MTX规则、YARA规则类型自定义。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 应用识别 | | 支持应用识别功能，包括：HTTP应用、IM文件传输、P2P下载、P2P音频、P2P视频、标准协议、财经软件、电子商务、工控物联网、即时通讯、加密隧道、软件更新、社交网络、数据库、网上银行、网络游戏、网页视频、网页音频、网络硬盘、网页邮箱、语音电话、远程控制、移动应用、其他应用等24种类型超过5000种应用识别。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 日志管理 | | 支持安全事件告警日志记录，告警类型包括：攻击检测、僵尸主机、WEB防护、异常流量、DDoS检测、加密流量检测、黑名单等。根据不同安全事件检测结果记录关键字段信息，包括但不限于：时间、五元组、级别、事件描述、响应码、攻击结果、源地址归属地、攻击主机国家、XFF、X-Real-IP、目的地址归属地、受害主机国家、动作、应用协议、应用、攻击类型、攻击阶段、攻击特征、研判特征、次数、请求头、响应头、响应体、VNI、MPLS标签、处置状态等信息；支持对全部或按条件搜索的安全事件进行二次聚合，包括事件描述、攻击主机、受害主机一种或多种聚合方式。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | ▲产品具有相关部门颁发的《国家信息安全测评信息技术产品安全测评证书》。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | ▲产品具有IPV6 Ready Phase-2金牌认证。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | ★产品具备《网络关键设备和网络安全专用产品安全认证证书》。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 5 | 出口链路汇聚交换机 | 端口数 | | ≥24个万兆SFP+，≥6个40/100GE QSFP28 |  |
| 包转发速率 | | ≥1620Mpps |  |
| 交换容量 | | ≥4.8/25.6Tbps |  |
| 模块数量 | | ≥4个万兆单模模块 |  |
| **（二)、北京市电子政务外网出口链路** | | | | | |
| 1 | 政务网出口防火墙 | 路由交换 | | ▲支持RIP、OSPF、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM；支持策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP/MAC绑定 | | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 地址转换 | | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 链路负载均衡 | | 支持链路负载均衡功能，支持轮询、加权轮询、就近选路、优先级、带宽比率等多种链路负载均衡算法，支持备用选路算法，支持链路过载保护。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DNS 双向智能转换 | | 防火墙作为 DNS 服务器可依据访问地址来源将服务器域名解析为内部地址或外部地址，同时支持通过配置多条转换策略，实现内网资源服务器的负载均衡。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 访问控制 | | 支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、数据库防护、防代理、APT等功能配置,简化用户管理；访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行Web认证，策略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略；提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析、宽泛策略分析，可在WEB界面显示检测结果。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 网络接入 | | 支持RADVD、ND、RIPng、OSPFv3、BGP4+，支持IPv6静态、动态组播路由；支持NAT64、NAT46、NAT66地址转换，支持6to4隧道、ISATAP隧道。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IPv6访问控制 | | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DDOS 防御 | | 支持 HTTP DDOS 防护，采用阀值检查、源/目的限流 、 源 认 证 、 会 话 限 制 等 方 式 综 合 进 行 HTTP FLOOD、HTTP URI CC 攻击、HTTP 连接耗尽等攻击防护；支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP QUERY FLOOD、NTPREPLY FLOOD 攻击防护。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资源虚拟化 | | 支持在一台物理设备上划分出128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于24个虚拟防火墙授权。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 功能虚拟化 | | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、僵木蠕、高级威胁防护、内容过滤、邮件安全、审计、报表、防代理等安全功能虚拟化。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资产管理 | | 支持管理员手动添加、批量导入、设备主动扫描、EDR资产上报、漏扫资产上报等多种资产信息获取方式，支持基于访问流量自动识别发现资产；支持对被控制端为内网资产的telnet、ssh、rdp等常用的远程控制协议进行跟踪，支持对内网资产提供socks5代理的情况进行跟踪。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 系统诊断 | | 支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP、HTTP、DNS诊断方式。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 审计 | | 支持独立审计策略，支持审计白名单；支持访问网站URL 地址、网页标题和网页内容审计；提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、FTP；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端IP、用户名、协议、上行流量、下行流量、总流量、时间等；支持基于应用、网站类型、用户对用户上网行为进行统计和排序；支持进行违规应用分析、违规网站分析、用户违规访问公示。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 日志 | | 支持日志外发至多个SYSLOG服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；日志存储模式支持空间模式和时间模式，时间模式下日志能够保存180天。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 联动功能 | | 支持与漏扫、EDR、DLP、WAF、防病毒网关、数据库审计设备联动，并提供信息产业信息安全测评中心、公安部信息安全产品检测中心、国家版权局、中国软件评测中心之中任意一家机构出具的相关证书或测试报告。 | （提供≥一份上述证书或报告复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | 产品需具备信息安全产品自主原创证明。 | （提供证明文件复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 产品资质 | | ★产品需具备网络关键设备和网络安全专用产品安全认证证书、网络安全专用产品安全检测证书。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| **二、内网安全设备** | | | | | |
| 1 | 堡垒机 | 功能参数 | | 1.支持限定不同的协议应用发布服务器节点访问不同的资源；多协议应用发布服务器节点可访问相同资源时实现自动负载均衡。 |  |
| 2.运维角色支持时间、命令和审批策略，支持角色克隆；支持用户、资源与角色关联，形成访问策略；可对访问策略进行增删改查；支持超过角色中时间策略中的时间范围，系统将阻断运维会话。 |  |
| 3.支持数据库协议自动改密，改密类型支持：Oracle、PostgreSQL、MySql、DB2、Informix、SYBASE、SQL SERVER。 |  |
| 4.支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告；支持管理员帐号设置双因认证、IP/MAC限制。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 5.支持 Oracle（支持ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata、DM6\7\8、KingBase、MongoDb、Redis、GBase、GaussDB、OceanBase、GreateDb、GoldenDB、AISWare AntDB数据库命令级审计及下行返回行数记录。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 6.支持FTP、SFTP、SSH、RDP、SCP等协议运维时，对传输文件进行留存。 |  |
| 7.支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果；支持通过搜索操作语句或执行结果中关键字定位审计回放。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 8.产品支持运维人员操作的全过程的记录与报告；内置USB-KEY认证、国密USB-KEY认证、动态口令认证、国密动态口令认证、手机令牌认证、http通用认证、webservice通用认证、超级SIM认证、邮件认证等身份认证方式；支持用户以手机号码或邮箱地址作为用户身份登录。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 9.支持HTML5运维与审计，无需安装插件；支持国产化运维终端调用应用发布工具运维，支持发布国产化运维工具，实现录像审计（RDP/VNC/X11/HTTP(S)/国产数据库等）； |  |
| 10.支持通过国产化与非国产化应用发布开启运维屏幕水印，运维本地无法篡改水印内容，提升运维过程数据安全性。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 11.运维用户可以设置自动运维操作定时/周期执行，实现网络设备配置的自动备份；支持管理员通过WEB界面自定义上传用户手册，保证使用手册及时更新。 |  |
| ★12.产品需符合《信息安全技术网络安全专用产品安全技术要求》和运维安全管理产品（增强级）相关标准规范要求。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 13.产品需具备《IT产品信息安全认证证书》。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 2 | 双因素认证 | 主体功能 | | 在账号、静态口令认证基础之上，增加动态口令和生物识别认证方式，在最基本的静态口令认证这一环节，部署双因素动态身份鉴别系统，提升全场景入口安全级别，防止恶意入侵或人为破坏等非法操作。 |  |
| 动态认证系统提供认证服务、资源管理、策略管理、账号管理、日志审计、集成动态令牌认证引擎、生物识别认证引擎和RADIUS、TACACS+、LDAP协议服务，支持windows或linux操作系统部署模式，支持双机容错；支持主流网络设备、操作系统、业务系统等场景对接 |  |
| 扩展性：兼容多种认证方式，包括硬件令牌、app令牌、短信令牌、PC令牌、H5令牌、微信令牌、指纹令牌等多种方法混合使用 |  |
| 资源管理 | | 业务系统、操作系统设备：需要配置设备名称、共享密钥、设备地址；可以定义选择设备类型、认证策略；可以一键开启地址校验、一键开启设备接入是否生效 |  |
| 认证终端设备管理，需要显示终端序列号、终端类型、终端地址；可以根据终端序列号进行查询，分页显示；支持新增、修改、删除操作 |  |
| 网络设备：需要配置设备名称、共享密钥、设备地址；可以定义选择设备类型、认证策略、授权策略、协议认证、Radius属性；可以一键开启多步认证、一键开启接入设备是否生效；支持华为云CHAP | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 认证策略 | | 同时为一个用户支持硬件令牌、手机令牌、短信密码、PC令牌、微信令牌、扫码认证等多种认证方式，支持用户的多种令牌混合使用 |  |
| 支持消息密码认证、静态密码认证、动态密码认证、推送认证、强认证、认证转发；支持消息令牌过滤；支持内部用户认证、外部用户源认证 |  |
| 可以自定义授权策略，自定义授权规则，自定义规则权限，Radius报文属性自定义 |  |
| 默认短信自动触发至用户预制手机上，无需填入手机号 |  |
| 支持策略组设置认证用户是否启用静态密码、动态密码、强认证开关键；支持强制部分用户或所有用户采用动态密码认证方式 |  |
| 策略组支持设定管理员，管理员可管理应用该策略组的设备 |  |
| 账号管理 | | 基于Web管理，实现账号以及组织架构统一管理，方便操作和使用 |  |
| 支持认证系统内建本地用户账号管理及树形组织架构展现；支持用户账号数据导入和导出 |  |
| 针对本地组织架构或者用户组下的用户，支持批量派发和绑定令牌、令牌导出、重置密码、认证策略设定 |  |
| 支持外部账号源，如AD/LDAP，数据库、API接口等账户源 |  |
| 支持本地角色的自定义维护管理；支持外部数据源角色的自动同步；支持针对角色所属用户是否开启使用消息令牌 |  |
| 支持单个用户设置认证策略，且单个用户认证设置优先于对接设备的认证策略；便于单个用户灵活认证配置认证策略 |  |
| 可设定用户绑定一种类型令牌个数控制，默认每个用户一个令牌，通过令牌备注用户个体；支持软件令牌激活码通过邮箱模式发送 |  |
| 支持自动生成应急动态密码，用于应急状态下使用 |  |
| 令牌管理 | | 能够直观显示令牌与账号的绑定关系、令牌类型等信息，具备对令牌生成的动态密码进行测试和校验；并支持根据令牌序列号进行查询，分页显示 |  |
| 令牌分发模式包括：模板下载、上传硬件令牌密钥文件、批量硬件令牌派发、消息令牌手动释放等操作 |  |
| 时间型令牌：支持软件令牌种子密钥加密算法类型（SHA1\SM3）；可以自定义软件令牌开头标识符；支持自定义动态密码的有效使用次数；允许用户选择动态密码变换周期（30/60秒） |  |
| 消息令牌：支持根据账号、手机号、微信等条件，选择接受动态密码的发送目标；支持自定义设置短信密码长度，短信验证码有效期时长 |  |
| 支持自助指纹注册功能，便于用户指纹注册采集； | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持一键启动全局短信令牌，并支持有效期内是否连续发送短信验证码 |  |
| 日志审计 | | 支持针对授权日志、审计日志、API认证日志、协议认证日志、终端日志、系统操作日志的管理 |  |
| 认证日志：通过标准协议对接的所有详细日志，包括账号、用户端IP地址、设备名称、设备地址、认证状态、认证详情、记录时间等； | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 所有日志审计记录，均支持导出功能；支持根据账号、设备地址等细粒度查询；支持分时间段、分页等条件查询等；能够做到溯源追踪 |  |
| 安全机制 | | 支持密码规则设定，可自定义设置最小密码长度、密码有效期 |  |
| 支持在首页面显示认证状态，是否存在异常 |  |
| 支持固定PIN码、灵活动态设置PIN码认证模式，与动态口令组合的方式进行认证；固定PIN码可以有管理员统一设置；动态PIN码支持灵活的设置方式。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持日志扩展，防止日志数据量过大造成日志查询性能降低 |  |
| 支持服务器所有日志信息上传Syslog日志服务器 |  |
| 支持Radius认证服务转发，自动学习，无需手动添加账号 |  |
| 系统自动化 | | 支持自动化清理超过3个月的历史记录、日志记录、操作日志，可自定义执行时间、运行间隔时长、启动延时时长； | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持无用软件令牌自动清理，可自定义执行时间、运行间隔时长、启动延时时长； |  |
| 支持一键开启是否放开自助登录服务功能，并支持设定用户自助维护的权限控制，允许/禁用用户自助绑定、解绑令牌； | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持定时、间隔批量发送软件令牌激活邮件，可自定义执行时间、运行间隔时长、启动延时时长； |  |
| 系统管理 | | 支持系统软件管理，支持添加系统用户并自定义设定系统用户权限 |  |
| 支持管理账号自身双因素认证 |  |
| 支持特定IP地址访问系统平台权限 |  |
| 能够直观显示授权信息：包括授权数量、令牌类型、授权日期等相关信息 |  |
| 支持系统邮件配置管理，支持邮件模板设定 |  |
| 支持短信平台对接、支持短信猫、短信网关；支持短信模板自定义；支持多种短信网关接口 |  |
| 支持通过web页面模式，实现系统在线升级，简化升级操作流程 |  |
| 令牌绑定 | | 支持60秒硬件令牌；支持30秒、60秒自变化手机令牌 |  |
| 手机令牌支持单位时间内激活有效，并可设定时间阈值 |  |
| 支持短信密码、手机令牌、硬件令牌、指纹令牌同时并存 |  |
| 手机令牌支持依据用户角色派发一个或多个用户 |  |
| 通过为AD/LDAP用户的特定属性字段添加硬件令牌序列号，实现硬件令牌/手机令牌自动绑定 |  |
| 支持动态口令有效期设定，支持手机令牌和消息令牌属性自定义 |  |
| 支持矩阵 | | 支持Citrix Netscaler，VMware vcenter、华为、Parallels、IBM等虚拟化场景 |  |
| 支持手机令牌、硬件令牌认证、微信小程序、H5令牌等方式认证 |  |
| 支持Juniper、Cisco、Array、F5、深信服、H3C、天融信等主流VPN场景 |  |
| 支持启明星辰、金盾、思福迪、帕拉迪、绿盟、齐治等堡垒机场景 |  |
| 支持Cisco、Huawei、H3C、中兴、锐捷、JUNIPER 等交换机场景 |  |
| 支持华为、华三、天融信、深信服、飞塔、安恒、360等防火墙场景 |  |
| 支持OA、ERP、金蝶、用友、HR、CRM、SAP、Oracle等业务系统集成 |  |
| 支持http/https 协议API，支持基于C、C、C++、.net、JAVA、PHP、python等各类语言开发的软件系统集成 |  |
| 支持Windows、Ubuntu、linux、CentOS、Suse等操作系统（在线、离线、应急）动态口令登录模式。 |  |
| 提供agent插件，支持Windows 桌面登录，并实现自动化配置 |  |
| 支持windows操作系统指纹认证； |  |
| 支持Weblogic管理帐号双因素认证 |  |
| 支持VNC远程连接双因素认证 |  |
| 硬件令牌 | | 令牌自保护防拆，令牌拆除自毁 |  |
| 算法要求：遵循国密SM3标准算法，符合国家标准。种子文件应该为64个字符。 | **（提供种子文件格式截图）未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 密码显示位数：6位、常显 |  |
| 密码变换周期：60秒，可以特殊定制30秒 |  |
| 指纹令牌 | | 采用业内优秀的光学设计，具有采集范围大、指纹图像像素高，干、湿、粗糙指纹效果好等优点。 |  |
| 按压次数≥400万次；指纹图像录入时间≤250ms |  |
| 对比模式支持：1:1，1:N 比对，支持分布式比对和集中式比对两种比对模式； |  |
| 手机令牌 | | 支持平台：IOS、Android、鸿蒙系统；支持各大应用商店下载 |  |
| 激活方式：支持帐号密码、扫描二维码与读图方式激活等方式激活令牌 |  |
| 安全性：支持设定手势密码、指纹或人脸识别，提高安全性 |  |
| 密码变换周期：30秒、60秒 |  |
| 推送认证：支持消息推送认证功能。 |  |
| 批量派发：支持按用户角色批量派发； |  |
| 时效性：二维码与激活图片具有时效性，可以支持自定义时效； |  |
| 扫码认证：支持扫码登录功能 |  |
| 资质证书 | | 产品具备商用密码产品认证证书，≥符合国家GM/T 0028《密码模块安全技术要求》，且证书在有效期内。提供证书复印件并盖厂家公章 |  |
| 产品具备IPV6 Ready logo 国际认证，提供证书复印件 |  |
| 产品取得相关部门颁发的信息技术产品安全测试证书，并经过漏洞库（更新至2023年1月1日之后）覆盖测试，不存在漏洞库中已知中、高风险漏洞。提供证书复印件 |  |
| 产品原厂具有发明专利证书，提供证书复印件 |  |
| 3 | VPN | 技术要求 | | 1.专业IPSec VPN和SSL VPN二合一设备，非插卡或防火墙带VPN模块设备。 |  |
| 2.支持多系统引导，可在管理员界面直接配置启动顺序，≥支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且分别支持加密导入导出；同时支持全局配置安全检查，支持一键优化或一键锁定。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 3.支持配置多种资源类型，包括WEB应用、WebVPN应用、TCP/UDP应用，NC应用；支持资源负载均衡，可控制终端接入类型，如PC端（浏览器/独立客户端）、移动端（Android/iOS）；支持WebVPN跨平台免插件访问，支持Windows、Mac、Linux、国产化UOS\银河麒麟V10等系统主流浏览器，免插件免客户端使用VPN接入内网。 |  |
| 4.支持网关、单臂部署模式，IPSec VPN支持透明、路由、冗余等网络接入方式；支持IPSec隧道组和隧道热备份；支持IPSec VPN隧道间路由实现隧道接力；支持IPSec手动隧道，手动输入密钥参数，建立隧道。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 5.支持短信认证，支持HTTP、WebService接口自定义。支持CAS认证服务联动，通过简单配置即可实现基于身份票据的单点登录；支持密码自助找回功能。 |  |
| 6.支持IPSec、SSL 、PPTP、L2TP VPN的统一用户管理和认证体系，实现用户名口令一次配置，即可适用于全部VPN类型接入。 |  |
| 7.支持全局抗攻击功能（包括抗地址欺骗、抗源路由攻击、抗SMURF攻击、抗LAND攻击、抗WINNUKE攻击、抗QUESO扫描、抗SYN/FIN扫描、抗NULL扫描、抗圣诞树攻击、抗FIN扫描、抗Ping of Death）支持基于包过滤规则的抗SYN FLOOD、抗UDP FLOOD、抗ICMP FLOOD和IP会话数控制。 |  |
| 8.基于用户和角色设定准入策略，针对操作系统、操作系统补丁、浏览器、进程、服务、端口、文件、注册表、登录IP、时间、凭证、终端指纹进行登录前和使用时定期检查。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 9.支持在Windows、统信UOS、银河麒麟等操作系统上远程应用发布B/S和C/S应用功能（非整个桌面进行发布），只传输鼠标、键盘操作和显示数据，无需安装CS客户端。 |  |
| 10.支持终端认证功能，包含硬件特征码、IP、MAC、主机绑定，特征码信息可自动生成，支持自定义用户绑定终端数量。支持硬件特征码批量导入导出；支持设定使用VPN时仅能访问内网资源，断开与对互联网的访问，支持登录超时限制时间功能。 | （提供证明材料，包括网站截图、功能截图、第三方检测报告中任意一种，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 11.采用加密方式建立隧道连接，支持自主隧道配置技术；具备基于SSL协议的远程安全接入方法和系统技术证书。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 12.产品需具备VSP通用安全平台软件，具备高效、智能、安全、易扩展等特点。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ★13.产品需符合《信息安全技术网络安全专用产品安全技术要求》和虚拟专用产品（增强级）相关标准规范要求。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 14.产品需具备国家密码管理局发布的《商用密码产品认证证书》。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 4 | 网络审计 | 内容审计 | | 支持对HTTP协议进行内容审计，审计内容包括不限于：访问域名，HTTP引用页、URL、HTTP请求类型、HTTP响应类型、请求文件、请求参数、访问行为、响应码、访问浏览器、服务器、Cookie、源目的IP地址、信誉分值等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持文件传输协议审计（FTP、TFTP协议），可针对FTP协议文件传输的网络行为进行审计，审计内容包括但不限于：文件名、操作命令、操作结果等，可以对上传下载的文件进行还原，提供下载。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 持共享协议（SMB 文件共享、NFS 共享）审计。包括不限于：用户名、操作命令、传输文件名/文件类型等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 行为审计 | | 支持应用协议行为识别，应用识别规则库最少分为24大类，支持5000种以上的应用协议自动识别与审计记录。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 告警阻断 | | 支持旁路模式阻断和防火墙联动方式阻断，支持与沙箱联动响应；支持Syslog、snmptrap、Kafka、Netflow、FTP、邮箱、短信、企业微信等方式向外发送告警日志。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IPv6环境 | | 支持IPV6环境部署和IPV6环境下网络审计系统全部功能的审计。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 审计查询 | | 支持标准查询、经典查询和专家查询多种查询方式。支持界面展示查询条件、事件数、应用协议及任务运行时间。支持以柱状图的形式展示各时间段审计事件数；支持自定义查询事件数，支持千万级数据秒级查询，支持csv格式导出审计日志。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 实名审计 | | 支持实名审计，支持绑定源IP、用户名，域名、主机名、部门、邮箱及电话，支持手动添加数据来源，或下载模板批量导入，并支持全量导入。支持在审计日志中实名相关信息区域，查看实名关联信息，展示用户名、域名、主机名等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 黑名单检测 | | 支持黑名单检测，支持黑URL、黑IP、黑域名、黑账号检测等审计策略，支持报文留存。支持黑URL地址、黑域名、账号多种匹配类型，包括子串匹配、左匹配、右匹配、完全匹配及正则匹配。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 攻击检测 | | 集成攻击检测规则库，支持对扫描探测、暴力破解、后门控制、溢出攻击、注入攻击等攻击行为检测告警，并且支持自定义攻击规则。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 僵尸检测 | | 支持对僵尸网络、木马控制、蠕虫、挖矿、勒索等僵尸规则的管理和侦听，并对攻击信息详细审计（攻击类型、操作系统、风险等级），可对风险主机进行取证、告警及阻断处置。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 异常流量检测 | | 支持异常流量检测，支持flood攻击检测、接口流量监测。支持配置异常连接检测周期、接口流量上限及总流量上线。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资产识别 | | 支持资产发现，支持指定网络中的在线资产识别, 支持主动监测，对网络中设备资产进行发现和梳理，能够对资产IP、资产状态、系统版本、开放端口进行安全监测。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 统计报表 | | 支持按协议或告警类型统计报表，以文字和图表的形式展示报表内容。支持WORD、PDF、OFD、EXCEL、HTML 等格式导出报表。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 系统告警 | | 支持系统状态阈值设置，包括不限于 CPU 阈值设置、硬盘空间阈值设置、内存空间阀值设置等，当使用率达到预定的阈值时，系统会发出报警。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 系统管理 | | 支持本地认证、Radius、LDAP等用户认证方式。支持双因子认证。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 探针部署 | | 对无法通过旁路方式进行镜像监听场景，支持多种类型操作系统的探针部署，适配的操作系统≥包括以下几种： AIX5/6/7、WinSer2003 /2008 /2012 /2016 /2019、Centos、opensuse、redhat、Ubuntu、麒麟、统信、凝思、普华等。 |  |
| 产品资质 | | ▲产品具有IPV6金牌证书。（提供证书复印件，并加盖制造商公章） |  |
| 产品资质 | | ▲产品具备中国信息安全测评中心颁发的信息技术产品安全测评证书EAL3+级以上。（提供证书复印件，并加盖制造商公章） |  |
| 产品资质 | | ★产品具有网络关键设备和网络安全专用产品安全认证证书。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
|  | 网络安全漏洞扫描系统 | 功能要求 | | 1.支持扫描的漏洞数≥400000个，支持IPv4和IPv6环境的部署和扫描。 |  |
|  |
| 2.支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、Debian、深度、红旗、麒麟、新支点等；支持对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、神通、达梦、人大金仓、优炫等。 |  |
| 3.支持对网络设备的识别与扫描，包括：Cisco、Juniper、华为、中兴、H3C、TPLINK、DLINK、F5、Checkpoint、Alcatel、三星、Symantec、Nortel、Linksys、ZyXEL等，能够扫描的网络设备漏洞扫描方法不小于5000种。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 4.支持对主流虚拟化软件平台的识别与扫描，包括：OpenStack 、KVM、Vmware、Xen、Docker、Huawei FusionSphere等。 |  |
| 5.支持对视频监控类设备的识别与扫描，包括大华、海康、宇视、雄迈、科达、TBK、NUUO、Samsung、Vivotek、Wanscam、Axis、Geutebrück、Keeper、Blink、CACAGOO等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 6支持对Apple系统和应用组件的识别与扫描，包括MAC OS、IOS、watchOS、Safari、itunes、iCloud、CUPS、QuickTime、libxpc、libxml2、sysdiagnose、Quick Look、ASN.1等，能够扫描的Apple系统和应用组件漏洞扫描方法不小于6000种。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 7.支持对Web应用系统的扫描，支持检测SQL注入漏洞、命令注入漏洞、CRLF注入漏洞、LDAP注入漏洞、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等。 |  |
| 8.支持对扫描对象的挂马、暗链、敏感词进行检测。支持网站风险监测，可以对网站可用性、网页变更、DNS地址解析进行监测，实时发现网站风险。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 9.支持针对网站漏洞进行问题点、问题参数描述，具备完整的测试用例来验证漏洞存在的真实性。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 10.支持配置变更检查，可以根据实际情况设置任意检查结果作为变更基线，支持与自身或者其他设备的同类型变更项进行对比，检查设备间核心配置项的异同之处。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 11.支持扫描任务参数设置，包括执行方式、执行时间段、任务模板、策略模板、扫描方法、任务优先级、插件超时时间、断网续扫、模糊扫描等。 |  |
| 12.支持资产拓扑功能，可自动生成资产拓扑图；支持按照部门、资产类型、IP分组等多种方式对所有资产进行展示。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ★13.产品需符合《信息安全技术网络安全专用产品安全技术要求》和网络脆弱性产品（增强级）相关标准规范要求。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 14.产品需具备《IT产品信息安全认证证书》级别EAL3增强级。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 6 | 态势感知平台流量探针 | 技术要求 | | 1.支持大屏展示能力，可通过大屏展示网络整体态势与趋势，支持对亚太版世界地图与中国地图展示进行切换，大屏安全汇总信息可下钻至具体数据。 |  |
| 2.支持支持深度协议解析包括http、https、dhcp、dns、ftp、mysql、imap、bgp、sip、pptp、l2tp等多种通用协议解析；支持gtpu、ngap、pfcp等5G协议及工控协议的解析；支持基于不完整会话流的单包攻击检测能力。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 3.支持导入HTTPS、POP3S、IMAPS、SMTPS、RDPS证书,对加密流量进行解密及还原，支持SSL3.0、TLS1.0/1.1/1.2。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 4.支持程序具备AI引擎自动对攻击进行威胁情报云查，页面自动呈现情报云查信息，查询结果≥包含：威胁等级、标签、威胁类型、IP地址、IP类型、活跃时间、发现时间、国家、地区、运营商、恶意端口等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 5.支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源IP、源端口、目的IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，兼容业界主流snort规则。 |  |
| 6.支持基于流量的实时IOC检测，检测类型包含：IP、域名、URL、文件Hash、JA3等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 7.支持通过web页面导入pcap包离线回放检测能力，支持导入pcap数量不少于100个；支持导入单个文件、批量导入多个文件、导入文件夹；支持对导入的pcap单独回放或批量回放。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 8.支持对终端、视频设备、办公设备、网络设备、服务器、安全设备、工控设备等资产类型自动发现；支持对资产的设备类型、操作系统类型、MAC地址、IP地址、端口服务等精准识别。 |  |
| 9.支持基于特征库检测挖矿主机，支持对挖矿主机进行连接矿池阶段、获取挖矿任务阶段、控制命令通信阶段、挖矿成功阶段，形成挖矿链可视跟踪。对网络中的挖矿主机活跃程度，挖矿币种有直观的图形化展示。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 10.支持通过syslog/kafka/SNMP trap方式将告警日志、违规互联日志、威胁情报日志、流数据日志、协议元数据外发至第三方数据采集平台，支持同时配置多个外发采集平台。 |  |
| 11.支持通过页面对告警前后存储报文数量进行配置，并支持启用或禁用情报检测、弱口令检测以及敏感信息检测的pcap包存储功能。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 12.支持设备系统管理，可通过页面下发诊断对设备关键进程进行监测，同时可一键恢复关键进程。 |  |
| 13.产品需具有网络入侵特征配制方法及配置系统；具有加快旁路入侵检测的方法及检测装置。（提供证明材料复印件，并加盖制造商公章） |  |
| ★14.产品需符合《信息安全技术网络安全专用产品安全技术要求》相关标准规范要求。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 15.产品需具备CVE、CNNVE兼容性资质证书。 | （提供证书复印件，并加盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 16.产品需具备《IT产品信息安全认证证书》级别EAL3增强级。 | （提供证书复印件，并加盖盖制造商公章）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| **三、IPv6协议转换平台** | | | | | |
| **序号** | **产品** | **功能要求** | | | |
| 1 | IPv6协议转换平台 | IPv6智能升级系统 | 翻译功能 | ▲IPv6翻译，支持IPv4和IPv6协议的双向翻译；**提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 2 |
| 内容升级，支持在IPv4和IPv6之间进行内容的处理如标识显示应答等； |  |
| 内容缓存，支持在IPv4和IPv6通道之上的内容池的管理和可控互通使用，大幅提高升级系统的吞吐能力； |  |
| ▲IPv6访问标识，能够为IPv6用户访问页面时提供IPv6标识展示，提示当前正在使用IPv6协议访问网站； | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 用户溯源 | ▲溯源分析，支持IPv4和IPv6用户溯源功能； | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 负载均衡 | 4层负载均衡，提供主备，主主等多种工作模式，自动检测并调度资源系统，提供异常资源秒级切换能力，同时负载均衡服务故障能够自动发现和剔除； |  |
| 7层负载均衡，提供应用层弹性负载均衡的能力，通过提供依据请求IP，请求头，请求会话等多个维度的负载均衡算法； |  |
| 域名解析 | 支持IPv4/IPv6智能地址解析和查询； |  |
| 支持在IPv4/IPv6双栈环境下DNS授权解析和递归解析； |  |
| 支持IPv4环境或纯IPv6环境下的A/AAAA记录解析； |  |
| 外链改造 | 支持外链协议升级，在单一IPv6 用户环境下可以访问IPv6 的外链网站并且没有天窗问题； |  |
| 支持自动发现网站已经支持IPv6 的外链域名，且对于已经支持IPv6 的外链智能不进行协议升级； |  |
| 支持设置单个域名的外链翻译开关功能，支持一健控制全部外链翻译的开关功能； |  |
| 支持手动添加外链白名单功能，对白名单外链接不进行翻译； |  |
| 支持可视化外链翻译开关，保证纯IPv6 用户访问网站页面与布局的一致性。 |  |
| 内容加速 | 支持自主制定缓存策略； |  |
| 支持自动或者手工方式刷新缓存； |  |
| 支持JPEG、GIF、MP3、MP4、WMA、ZIP、RAR、FLV、LETV、F4V、EXE、ISO、APK、XML、CSS、JS资源的缓存，支持永久缓存、不缓存或短期缓存和分段缓存； |  |
| 具备全局负载均衡和智能调度，可自主制定缓存策略，根据策略自动选择时延最短、节点负载最轻的传输路径，将用户的请求导向整个网络中的最佳节点，为客户提供稳定、优质的加速服务。 |  |
| 集群管理 | 支持集群中设备支持自定义角色，≥包括：配置服务器、业务服务器、日志服务器，配置服务器支持主备设备； |  |
| 支持不中断业务下的设备级扩容，集群支持主备模式和负载均衡模式； |  |
| 支持网络发布服务负载均衡模式调整，包括稳定模式、根据连接数、流量或者源地址进行负载均衡； |  |
| 支持基于服务状态、网络状态、端口状态的集群负载切换，自动剔除集群中存在故障的设备，保证业务连续可用性。 |  |
| 协议升级 | 支持将HTTP协议的网站升级为HTTPS协议的能力； |  |
| 支持将HTTP1.0/1.1协议的网站升级为HTTP2协议的能力 |  |
| 支持主流网站采用的所有协议，包括HTTPS等，支持4A模式升级（IPv6与IPv4网站同域名），改造网站的二级、三级链接均能保证正常访问，并且保证支持网络购物网络银行等电子商务、在线视频、聊天软件等页面内容； |  |
| 支持多域名或多网站共享IPv4地址；支持多域名或多网站共享IPv6地址； |  |
| 支持对源站死链的智能优化，如400 转200； |  |
| 支持HTTP ALG应用层转换、FTP ALG应用层转换；支持HTTP、HTTPS、POP3、SMTP、IMAP, RTCP、RTSP、MMS, XFF等协议； |  |
| 访问控制 | 黑白名单，支持基于IP地址以及IP段的访问控制能力 |  |
| 访问限速，支持≥6种标准特征下的访问频率控制能力 |  |
| 源站保护 | 负载均衡，支持多个源IP情况下的自动负载均衡能力 |  |
| 异常调度，支持多个源IP情况下单源质量下降甚至服务中断情况下的无损切换能力 |  |
| 有序回源，支持在高并发情况下的回源队列控制能力，避免源站被大量并发请求冲垮 |  |
| ▲应急快照服务，在站点维护期间，通过快照对外提供服务保障。 | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 证书 | ▲**提供相关系统相关的软件著作证书，并加盖供应商公章** |  |
| 3 | IPv6  WAF安全防护系统 | 安全防护 | 五元组过滤：支持IPv4和IPv6五元组（源地址、源端口、目的地址、目的端口、协议类型）过滤防护； |  |
| ▲七层防护：支持http七层防护功能（平台级WAF），防止Web入侵及数据泄露； | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 0day攻击防护：基于漏洞预警+规则提取进行未知攻击拦截； |  |
| ▲防盗链：支持防盗链，防止站点元素或者连接被盗链； | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| ▲URL校验：支持对Url进行校验功能； | **提供工信部或国家认可的检测机构检测报告复印件,并加盖供应商公章** |
| 防扫描：通过访问频率、访问请求头信息，访问IP，访问内容进行智能识别，对扫描流量进行阻断； |  |
| 监测报警 | 安全报警：通过大数据分析平台对云端攻击数据进行分析，提取攻击特征，进行安全事件关联分析； |  |
| 网站可用性监控：对网站进行HTTP/HTTPS监控、PING监控，分布于不同地区节点实时获取响应码和请求详情，进行监控； |  |
| 离线分析 | 1）离线分析：对日志进行离线分析、机器学习，对未知攻击进行拉黑处理； |  |
| 2）离线展示：对防护日志进行处理，生成可视化页面展示； |  |
| 其他辅助功能 | 1）审计取证能力：保存半年存储日志，支持常见的HTTP字段查询，支持ELK查询 |  |
| 2）隐藏源站IP：对源站系统信息、版本信息以及中间信息进行隐藏 |  |
| 3）情报收集能力：收集IP地址库、HTTP代理库、VPN库，具有黑白名单处理功能 |  |
| 4 | IPv6防DDos攻击服务系统 | 系统功能 | 1.支持 TCP/HTTP/HTTPS 及最新的 HTTP/2 协议,HTTPS 全链路支持； |  |
| 2.支持保护网站、应用程序和整个网络，同时确保合法流量的性能不受影响； |  |
| 3.提供转发规则数 60 个； |  |
| 4.支持IP/域名的黑白名单，域名自动检测； |  |
| 5.支持自定义防护策略； |  |
| 6.支持流量清洗数据统计与分析、攻击事件详细记录，支持生成数据； |  |
| 7.支持完整的记录攻击事件的各种元素，方便客户分析和了解攻击状态,实现攻击溯源； |  |
| 5 | 运维服务 | 配置系统 | 针对客户的配置进行管理配置，以及对服务器上的软件和配置进行管理，包括IPv6客户配置系统、软件配置管理系统。 |  |
| 部署系统 | 对接入IPv6云服务的网站应用部署相关服务器的软件升级、配置更新等部署操作进行管理。 |  |
| 监控系统 | 通过部署监控服务，针对接入网站的运行状态、可用性等监控，并将信息进行汇总分析，生成告警信息。 |  |
| 数据分析 | 提供访问数据分析。包括对客户的访问日志进行各种分析，对客户的使用流量进行统计。分析项目包括源站访问流量、IPv6用户请求数、用户请求状态码以及运营商分布。 |  |
| 6 | 检测服务 | 网站IPv6支持度检测服务 | 网站 IPv6 支持度深度检测服务及每月提供检测报告，服务器3年，检测项如下： |  |
| 1.网站域名 IPv6 地址解析能力 |  |
| 2.网站首页 IPv6 可访问 |  |
| 3.网站首页 IPv6 访问成功率 |  |
| 4.网站首页内容 IPv6 和 IPv4 的一致性 |  |
| 5.网站首页布局 IPv6 和 IPv4 的一致性 |  |
| 6.网站域名具备完整的 IPv6 域名授权体系 |  |
| 7.网站二级链接 IPv6 支持率 |  |
| 8.网站三级链接 IPv6 支持率 |  |
| 9.网站域名解析时延 |  |
| 10.网站首页访问时延 |  |
| 11.网站 IPv6 可访问稳定性 |  |
| 证书 | ▲**提供相关检测平台系统相关软件著作证书,并加盖供应商公章** |  |
| **7** | 维保期限 | 三年免费维保 | | | |
| **四、域名及地址管理分配部分** | | | | | |
| 1 | 统一管理节点 | 管理功能 | | 多节点统一管理支持节点位置图形化灵活编排，支持图形化区分节点角色（管理节点，服务节点）。 | （提供第三方检测机构出具的CNAS或CMA测试报告证明并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 因节点异常或网络等异常时，配置无法正常下发至全网业务节点时，可以通过网管查看每个节点队列中的指令。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持节点快速克隆的功能，因业务发展需要增加新的节点时，可以选择当前集群中已有的一台节点配置快速克隆至新节点，提升运维效率 |  |
| 管理功能 | | 中央管理设备主/备/从高可靠部署，主/备/从管理中心均须支持HA双机热备。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持配置服务级HA，包括不限于对DNS服务状态、DHCP服务状态、监听网卡等设置切换条件，从而保证业务更可靠。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持通过页面查看HA两台设备的同步状态，并可以手动开启/停止两台设备的数据同步，并能一键式切换HA主备关系 |  |
| 管理功能 | | 支持对系统消息或告警快速提醒功能，当有系统关键告警产生时，在页面中有明显提示告警条目，并可以提供快速查看的方法，不需要登录对应的告警模块即可第一时间处理系统关键消息。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持审核工作流，审核人员可对被审核人员在DDI系统中所有的新建，编辑，删除，批量变更等操作进行审批，审批结果支持邮件通知，且可指定审核人员与被审核人员的对应关系，审核记录支持追溯。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持账户分权，可设定基于视图、区、权威记录类型、单独权威记录的隐藏/只读/读写权限；支持账户分权，可设定基于网络/地址池的隐藏/只读/读写权限。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | Web前台界面支持启用抓包，可指定节点进行抓包并下载，帮助用户获取运行真实数据分析和处理问题。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持二级域名注册，管理员可通过动态增删申请项定制域名申请表，支持对申请域名可设置生效期限、变更域名属主、一键禁用所有或特定注册域名、配置允许用户自助维护注册域名或审核变更过程。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持为权威记录等资源列表动态添加自定义属性列，方便用户为域名记录灵活添加备注信息；支持为网络、地址池等资源列表动态添加自定义属性列，方便用户为网络、地址池灵活添加备注信息。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 管理功能 | | 支持通过web前台查看集群内所有节点的授权类型、有效时间、授权功能范围、授权凭证等；支持通过console口连接设备修改前台超级用户密码；支持不同license类型的节点统一纳管。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | 应用状态探测变更、多个探测模板中任一探测状态变更、节点间信息同步时连接状态变更均支持告警；支持对单个服务器单独配置探测协议，也可以通过资源池对引用的服务器指定公共的探测协议；支持探测节点间有冗余机制，当主用探测节点异常时可以由其他探测节点或者备份探测节点自动接替服务；支持域名级设置动态兜底的失败应答策略，减少人工重复配置。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | 支持通过API的方式整合第三方检测平台的业务状态，并可以基于第三方平台返回的业务状态动态切换域名。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | 支持自定义探测设备关联自定义健康检查模板对服务成员进行拨测，多个探测设备可以跨数据中心组成探测组，当选择多个探测设备组成探测组时支持轮询和全局可用的探测策略。支持对探测失败容忍时间进行设置，即探测失败时间超过容忍时间时才会对解析产生影响，不因某一个探测任务的结果进行判定。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | ▲支持域名解析数据的动态建模算法，可根据域名的解析分布时间、解析类型、解析频率等因素给出参考解析行为的“基线”值，当解析的相关指标超过此基线时，能给相关事件的态势预警提示。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | 提供智能化的访问调度功能，支持解析记录轮询返回，实现智能全局负载；支持会话保持自定义保持时间；支持IPv6数据中心调度策略；支持组合算法；支持静态就近性算法、全局可用性算法。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | 支持≥14种健康监测方式ICMP、UDP、TCP\_SYN、HTTP、HTTPS、TCP、FTP、SMTP、SNMP、SNMP\_LINK、TCP\_KEEP、DNS、MYSQL、ORACLE等。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | ▲支持增强应用状态获取的可靠性，数据中心应用服务成员健康状态通过仅本地数据中心、优先本地数据中心、同时多数据中心多种策略探知。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 智能解析 | | ▲支持转发服务器分组；支持对转发服务器健康状态进行监测，支持对异常服务器进行复检，保证异常服务器恢复后快速可用；支持递归请求失败时到指定服务器进行查询测试；支持EDNS携带映射源地址。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 解析拨测 | | ▲支持解析拨测，可进行批量域名的拨测和多DNS间解析一致性对比；支持解析状态监控，可对内网域名解析情况监控，解析延迟、解析结果准确度、解析异常等指标进行实时拨测；支持事件诊断功能，可基于拨测监控诊断数据，定位内网解析故障位置。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP地址管理 | | DHCPv6地址下发支持动态前缀，支持DHCPv6无状态地址下发（下发信息方式包括动态前缀和固定前缀两种方式）。 | （提供第三方检测机构出具的CNAS或CMA测试报告证明并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP地址管理 | | ▲支持EUI-64算法，支持DHCPv6下的EUI-64地址下发，且后缀地址生成基于EUI-64算法进行。 | （提供第三方检测机构出具的CNAS或CMA测试报告证明并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP地址管理 | | ▲支持创建IPv6地址规划方案并设置固定前缀。支持在地址台账中应用IPv6规划方案，可以便捷添加IPv6网络。支持通过规划地图直观展示全网的IPv6地址规划情况。 | （提供第三方检测机构出具的CNAS或CMA测试报告证明并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| IP地址管理 | | ▲支持按照图形化方式拖拽规划IPv6地址空间，且每个空间标记不同的业务类型。支持为各地址空间配置空间标识，同时关联与上级标识并形成可落地的IPv6编址方案。 | （提供第三方检测机构出具的CNAS或CMA测试报告证明并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 日志与分析 | | ▲支持全网运行状态实时监控；能够实时监测全网设备如下指标的总体统计：域名排行、查询IP排行、解析状态统计、解析类型统计、QPS、解析成功率、缓存命中率。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 日志与分析 | | ▲提供丰富的数据报表，可追溯所有失陷主机以及关联威胁信息，统计；支持对全网发现的所有失陷主机统计，以及失陷主机关联的威胁类型，发现时间统计；支持访问的情报域名TOP统计、以及每个域名关联的源IP TOP，情报上下文信息，情报信息包括威胁类型，严重级别，防护策略等。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 告警功能 | | ▲支持告警阈值设置，支持邮件、回调、SNMP、Syslog、短信、声音等告警方式，所有告警信息均支持设置不同的告警级别，包括但不限于Debug、Info、Notice、Warning、Err、Crit、Alert等。 | （提供满足功能场景需求、配置逻辑清晰且配置结果生效的产品界面截图并加盖制造商公章。）**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 资质要求 | | ▲所投产品须具备由国家保密科技测评中心颁发的涉密信息系统产品检测证书。 |  |
| 资质要求 | | ★所投产品须具备由相关部门颁发的网络安全专用产品安全检测证书。 | 列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 2 | DNS服务节点 | 技术要求 | | 支持节点位置图形化灵活编排、图形化区分节点角色，多节点统一管理；支持多管理/数据中心冗余；支持对不同用户组统一的分权管理；支持HA模式主备管理模式。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持域名分级分层配置下发，支持对三级及以上域名进行WEB网管，且下级单位DNS节点可以作为本级域名管理节点的同时承接上级管理平台下发配置项（配置项包括上级域名授权、本级DNS域名、DNS视图、本节点账号管理权限）。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持二级域名管理、注册、申请、变更、注销；对支持记录的解析日志信息保密；操作日志和系统日志对某些管理员不可见；具备灵活的数据报表分析能力，提供自定义报表功能，提供报表定制，可自定义数据统计报表。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持节点集中管理，支持运行信息同步展示，下级节点的运行信息可以实时同步到上级管理平台展示（展示信息包括：CPU使用率、CPU温度、内存使用率）；支持前台配置的备份和恢复；集群管理能力，具备域名系统集群统一管理中心平台，管理平台具备多级冗余技术能力。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲所投设备支持辅区永不过期；权威区支持12种记录（A、AAAA、NS、MX、CNAME、NAPTR、SRV、PTR、TXT、DNAME、SPF、CAA）类型添加/修改；支持权威主区；支持IPv4、IPv6反向区域；支持主辅区一键切换；支持权威记录资源自定义标识管理；共享区创建/编辑/删除；支持记录的联动删除PTR。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持转发服务器分组；支持对转发服务器健康状态进行监测，支持对异常服务器进行复检，保证异常服务器恢复后快速可用；支持基于源地址递归查询；支持对解析结果替换；支持EDNS携带映射源地址。 |  |
| 支持≥14种健康监测方式ICMP、UDP、TCP\_SYN、HTTP、HTTPS、TCP、SMTP、SNMP、SNMP\_LINK、DNS、TCP\_KEEP、MYSQL、ORACLE等。支持活跃地址功能，正常活跃地址解析，服务节点数量在限制区间中，解析结果可以正常返回；支持自定义设置探测组，设置内容包含探测策略、探测设备、且多设备之间探测结果相互同步，探测节点相互冗余。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持增强应用状态获取的可靠性，数据中心应用服务成员健康状态通过仅本地数据中心、优先本地数据中心、同时多数据中心多种策略探知。提供更多智能解析线路支持能力。支持NXDOMAIN转换功能，权威解析支持NXDOMAIN转换为NOERROR，递归同样支持NXDOMAIN转换为NOERROR。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持自定义探测设备关联自定义健康检查模板对服务成员进行拨测，多个探测设备可以跨数据中心组成探测组，当选择多个探测设备组成探测组时支持轮询和全局可用的探测策略。支持对探测失败容忍时间进行设置，即探测失败时间超过容忍时间时才会对解析产生影响，不因某一个探测任务的结果进行判定。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持解析拨测，可进行批量域名的拨测和多DNS间解析一致性对比；支持解析状态监控，可对内网域名解析情况监控，解析延迟、解析结果准确度、解析异常等指标进行实时拨测；支持事件诊断功能，可基于拨测监控诊断数据，定位内网解析故障位置。需提供产品界面截图。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲支持全网运行状态实时监控；支持设备关键运行统计、支持设备告警。支持智能化访问调度域名图形化展示，支持图形化展现域名的调度逻辑和资源状态。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲支持DNS配置导出，前台可以一键导出DNS配置项进行快速备份（导出的数据包含但不限于：视图配置、区配置、域名记录配置、转发配置、域名调度对象、本地安全策略）。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 3 | DHCP/IPAM服务节点 | 技术要求 | | 支持对IPv6网络进行增删改查，支持IPAM双栈，支持DHCPv6 option强制下发，支持配置IPv4及IPv6地址池有效截期。支持RADIUS及LDAP远程认证、支持基于MAC的本地认证。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持通过IPAM系统自动生成IPv6地址，在指定的地址区间内正序、倒叙、随机的生成地址，并支持设置生成的IP地址个数。支持对网络设备探测发现未管理的IP地址，并能通过邮件的方式发送告警通知管理人员。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲提供MAC地址访问控制功能，提供MAC地址黑白名单功能；提供Option访问控制功能，支持自定义Option控制规则，规则策略包括等于、不等于、包含、不包含等。支持IPv4及IPv6的DHCP Failover技术，支持调整MCLT和分担比例。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持IPv4与IPv6租赁日志展示时间、MAC地址、主机名、类型、DHCP Relay网关、网关地址IP、Request源地址、服务器回复IP、租期开始时间、租期结束时间等属性。IPv4和IPv6租赁日志支持Syslog配置和导出功能。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲支持网络IP使用率、已经使用地址数和地址总数的统计展示，以图形和列表的形式展示网络、IP地址，便于进行直观的网络地址管理。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲支持对IPv6的DHCP报文类型solicit、advertise、request、confirm、renew、rebind、reply、release、decline、information报文实时统计，可查看近三个月的统计数据，统计结果支持导出为PDF或CSV格式文件。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 提供中文图形化方式的全局所有子节点监控功能，包括但不限于：服务器性能、运行状态等。 | **提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或产品白皮书或第三方机构检验报告或其他相关证明材料，并加盖制造商公章。未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| ▲提供告警阈值设定功能，支持邮件、SNMP、回调、短信等告警方式，所有告警方式都支持设置不同的优先级。 | 需提供产品界面截图等证明材料。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| DHCPv6地址下发支持动态前缀，支持DHCPv6无状态地址下发（下发信息方式包括动态前缀和固定前缀两种方式）。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明，**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持EUI-64算法，支持DHCPv6下的EUI-64地址下发，且后缀地址生成基于EUI-64算法进行。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明，**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持创建IPv6地址规划方案并设置固定前缀。支持在地址台账中应用IPv6规划方案，可以便捷添加IPv6网络。支持通过规划地图直观展示全网的IPv6地址规划情况。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明，**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |
| 支持按照图形化方式拖拽规划IPv6地址空间，且每个空间标记不同的业务类型。支持为各地址空间配置空间标识，同时关联与上级标识并形成可落地的IPv6编址方案。 | 提供第三方检测机构出具的CNAS或CMA测试报告证明。**未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。** |

**（五）采购标的需满足的服务标准、期限、效率等要求；**

1、技术方案要求

（1）详细阐述本次改造的设计方案，包括需求分析、总体设计，详细设计、产品选型等；

（2）详细阐述项目实施方案，需详述项目施工组织方案，实施步骤、施工进度表、集成服务细节，测试、验收等。

（3）需对项目的重点、难点进行分析，并提出解决方案。

2、项目实施要求

1）项目管理要求

* 在合同生效以后，对采购人认为其能力与本项目所要求的能力不相称而提出更换的项目负责人或者技术员，中标方必须予以更换；中标方更换项目主要负责人或主要技术骨干必须书面报业主同意后方可进行。
* 项目实施过程中，如出现因实际情况需要修改技术或调整设备的，中标方要立即组成现场处理小组，小组负责人由采购方负责人和中标方项目负责人担任，中标方必须有≥一名以上技术骨干担任小组成员；中标方必须在最短时间内提交整改方案，如整改方案仍不能顺利解决问题，则采购人有权要求更换中标方技术骨干或项目负责人，中标方应全力配合。
* 项目实施完毕后，中标方要提供详实准确的竣工报告，报告内容要涉及项目中所有软硬件指标及技术实施细则，要求报告思路清晰、条理性强以及高可读性，采购人有权将不符合要求的竣工报告发回中标方重写；最终成文的竣工报告要求有纸质版本，并且要求有双方签字确认，留档保存。
* 集成商要对招标人进行系统培训等工作，并提交相关培训技术文档。

2）项目周期要求

* 中标方的项目实施时间计划必须满足以下要求：签订合同后90天内完成，期间要完善实施方案，包括绘制详细施工图纸，制定详细施工计划，安全措施等，并向招标人汇报，待实施方案经招标人确认后，才能够开始实施
* 项目实施必须严格按照实施计划及时间表进行，不得出现拖拉现象，如果实施过程中出现因技术难点导致未能按照计划执行的情况，则酌情延长实施时间并调整时间表；整体实施完毕后,交付用户试运行，试运行周期为1个周。
* 试运行开始同时，中标方开始着手编写竣工报告，要求报告在1个星期之内完成首稿。

**（六）采购标的的验收标准；**

由甲乙双方共同组织验收，具体内容包括：

1. 供货清单
2. 竣工资料
   1. IP地规划表
   2. 网络拓扑图
   3. 交换机配置表，包括管理地址、路由地址、Vlan划分、config文件等，每台设备一份。
   4. 网络安全设备配置表
   5. 项目设计及实施方案等
3. 测试报告
4. 双栈功能测试，包括核心层到各个出口链路，核心层到汇聚层、汇聚层到接入层，终端到接入层。
5. 所有安全设备功能测试
6. 域名解析及地址管理与分配系统功能测试
7. 业务连续性功能测试
8. 全网路由测试

**（七）采购标的的其他技术、服务等要求。**

1、培训要求

（1）使甲方受训的技术人员能够了解和熟悉整个项目设计思路。

（2）使甲方受训的技术人员能够了解和熟悉整个项目中所有新增的软硬件产品的原理及性能，掌握配置、调试、维护和排除故障的基技能，使技术人员能够熟练地操作和管理软硬件，可根据业务需要灵活配置系统用户、分配数据权限及重要数据的备份还原工作。

（3）投标人须详细阐述培训的内容、方法、时间、教材、费用等事项。

2、售后服务要求

1)服务内容

* + 工程竣工并通过最终验收后起，供应商对投标范围内的所有系统提供1年免费维护服务。
  + 设备售后保修服务期：本次招标采购的设备,设备原厂商提供的质保期不足3年的，质保期限为3年；设备原厂商提供的质保期超过3年的，按设备原厂商提供的质保期执行。
  + 属于保修范围、内容的项目，供应商要提供7天×24小时服务，在该期间接到使用方发出的故障通知后，应在2小时内做出故障响应，并在4小时内到达现场，8小时内排除故障。
  + 在1年服务期内，供应商应免费提供备品备件以供系统正常使用。
  + 在售后保修服务期内，供应商无偿提供人员和技术支持，配合使用方进行技术改进和升级。

2)服务方式

要求提供多种服务方式，包括：

（1）热线电话：提供7×24小时热线电话支持，随时解答设备及系统平台使用过程中出现的问题；

（2）WEB方式：提供7×24小时电子邮件、讨论组、文档下载等方式的远程技术支持；

（3）现场服务：提供7×24小时现场服务。

3)技术资料提供**（投标人自行承诺，格式自拟）**

原则要求（纸质和电子）

投标人提供的全部技术资料必须用中文编写，资料必须准确、清楚、完整，必须满足安装、调试、运行、维护的需要，并与移交时的系统环境一致。

资料清单：

设计及实施方案；（纸质和电子）

竣工资料；（纸质和电子）

系统培训文档；（电子）

硬件产品包装内的全部资料。