

克东县公共资源交易综合服务中心

竞争性谈判文件

项目名称：网络等级保护二级设备

项目编号：**[230230]KDC[TP]20210009**

第一章竞争性谈判邀请

克东县公共资源交易综合服务中心受克东县财政局的委托，采用竞争性谈判方式组织采购网络等级保护二级设备。欢迎符合资格条件的国内供应商参加投标。

一.项目概述

1.名称与编号

项目名称：网络等级保护二级设备

批准文件编号：克东财购核字[2021]00023号

采购文件编号：[230230]KDC[TP]20210009

2.谈判内容

包号	货物、服务和工程名称	数量	采购需求	预算金额（元）
1	网络等级保护二级设备	1	详见采购文件	718,000.00

二.参加竞争性谈判的供应商要求

1.供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件。

2.到提交响应文件的截止时间，供应商未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。（以通过查询“信用中国”网站和“中国政府采购网”网站的信用记录内容为准。）

3.本项目的特定资质要求：

合同包1（网络等级保护二级设备）：无

三.获取招标文件的时间、地点、方式

1.获取谈判文件的时间：详见谈判公告。

2.获取谈判文件的地点：详见谈判公告。

3.谈判文件获取方式：供应商须在公告期内凭用户名和密码，登录黑龙江省政府采购网，选择“交易执行-应标-项目响应”，在“未参与项目”列表中选择需要参与的项目，确认参与后即可获取谈判文件。

其他要求

1.本项目如采用“现场在线开标”模式进行开标，投标人需到达开标现场。

2.本项目如采用“不见面开标”模式进行开标投标人无需到达开标现场，开标当日在投标截止时间前30分钟登录黑龙江省政府采购网进行签到，选择“交易执行-开标-供应商开标大厅”参加远程开标。请投标人使用投标客户端严格按照招标文件的相关要求制作和上传电子投标文件，并按照相关要求参加开标。

3.本项目将采用电子评标的方式，为避免意外情况的发生处理不及时导致投标失败，建议投标人需在开标时间前1小时完成投标文件上传，否则产生的一系列问题将由投标人自行承担。

四.谈判文件售价

本次谈判文件的售价为 无 元人民币。

五.递交响应文件截止时间、开标时间及地点

递交响应文件截止时间：详见谈判公告

谈判地点：详见谈判公告

评审时间：详见谈判公告

开标地点：详见谈判公告

六.询问提起与受理

项目经办人：任女士 电话：0452-5657455

七.质疑提起与受理：

1.对采购文件的质疑按要求以书面形式提供纸质材料：

项目经办人：任女士 电话：0452-5657455

2.对评审过程和结果的质疑按要求以书面形式提供纸质材料：

质疑经办人：郭朗 联系方式：13634836998

八.联系方式：

1. 采购代理机构

采购代理机构名称：克东县公共资源交易综合服务中心

地址：克东县人和路40号中国农业发展银行（克东县支行）后院西侧

联系人：任女士

联系电话：0452-5657455

账户名称：系统自动生成的缴交账户名称

开户行：详见供应商须知

账号：详见供应商须知

2. 采购人信息

采购单位名称：克东县财政局

地址：克东县保安街圣水路18号

联系人：郭朗

联系电话：13634836998

克东县公共资源交易综合服务中心

第二章 采购人需求

一、项目概况：

本项目是按照《黑龙江省财政厅关于做好全省财政专网网络安全等级保护工作的通知》（黑财函【2021】202号）的要求，加强全省财政网络安全工作，保障预算管理二级等保系统安全稳定运行，特别是确保财政支付电子化安全管理，按照省厅提供的标准要求，我县需采购网络等级保护二级设备及2台防毒墙，加强网络安全运营。

合同包1（网络等级保护二级设备）

1.主要商务要求

标的提供的时间	合同签订后30个日历日内交货
标的提供的地点	黑龙江省齐齐哈尔市克东县财政局圣水路18号
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例100%，项目验收合格后一次性付清
验收要求	1期：符合《黑龙江省财政厅关于做好全省财政专网网络安全等级保护工作的通知》中二级等保要求
履约保证金	不收取
其他	现场踏勘时间、地点、售后、质保期、联系人、联系方式：1、踏勘时间1月30日 2、地点克东县财政局 3、联系人郭朗、联系电话18945211201 4、质量保证自安装日起至2023年1月，期间出现质量问题应及时更换或维修 5、售后服务自安装日起至2023年1月，如有技术操作及时远程操作或电话指挥操作 6、提供自安装日起至2026年1月期间所有软件更新升级服务。

2.技术标准与要求

序号	核心产品 （“△”）	品目名称	标的名称	单位	数量	分项预算单 价（元）	分项预算总 价（元）	面向对 象情况	所属 行业	招标技 术要求
1		其他交换设备	其他交换设备	台	200	63,000.00	126,000.00	否	-	详见附件一
2		入侵防御设备	入侵防御设备	台	100	50,000.00	50,000.00	否	-	详见附件二
3		漏洞扫描设备	漏洞扫描设备	台	100	150,000.00	150,000.00	否	-	详见附件三
4		其他计算机设备及软件	其他计算机设备及软件	套	100	38,000.00	38,000.00	否	-	详见附件四
5		其他交换设备	综合日志审计	台	100	113,000.00	113,000.00	否	-	详见附件五

序号	核心产品 ("△")	品目名称	标的名称	单位	数量	分项预算单 价(元)	分项预算总 价(元)	面向对 象情况	所属 行业	招标技 术要求
6		其他交换设备	堡垒机	台	1. 0 0	110,000.00	110,000.00	否	-	详见附 表六
7		其他交换设备	网络准入	台	1. 0 0	63,000.00	63,000.00	否	-	详见附 表七
8		服务器	终端安全管理	套	1. 0 0	68,000.00	68,000.00	否	-	详见附 表八

附表一：其他交换设备

参数性质	序 号	具体技术(参数)要求

1	<p>1、设备支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>2、设备具备链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。</p> <p>3、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>4、设备具备与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理。</p> <p>5、设备具备安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。</p> <p>6、设备具备策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。。</p> <p>7、设备具备多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。</p> <p>8、设备具备三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色。</p> <p>9、网络层吞吐量≥3G，应用层吞吐量≥600M;IPS吞吐量≥150M，防病毒吞吐量≥250M，并发连接数≥80万，HTTP新建连接数≥1.8万。接口：≥6千兆电口。</p> <p>10、设备具备不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>11、设备具备多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。</p> <p>12、设备具备全面的URL分类库，针对网站类别实现细粒度管控，杜绝非法、违规网站的访问行为。</p> <p>13、设备具备对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。</p> <p>14、设备具备对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置。</p> <p>15、设备具备病毒例外特征设置，根据文件MD5值和文件URL设置病毒白名单，不对白名单进行病毒查杀。</p> <p>16、设备具备勒索病毒检测与防御功能。</p> <p>17、设备支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。</p> <p>18、设备支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表二：入侵防御设备

参数性质	序号	具体技术(参数)要求
------	----	------------

	1	<p>1.产品支持NAT64和NAT46 地址转换方式，满足IPv6改造要求。</p> <p>2.产品支持多种用户认证方式，用户认证方式要求支持本地密码认证、外部密码认证和单点登陆等方式。</p> <p>3.产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能。</p> <p>4.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>5.产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。</p> <p>6.产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。</p> <p>7.网络层吞吐量≥3G，应用层吞吐量≥600M，并发连接数≥80万，HTTP新建连接数≥1.8万。1U机架式设备，单电源，接口≥6千兆电口。需具备web层应用防护能力。</p> <p>8.产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。</p> <p>9.产品支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。</p> <p>10.产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。当主机进行合法外联时，支持对不少于9800种应用的识别和控制。应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>11.产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。</p> <p>12.支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。</p> <p>13.支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。	

附表三：漏洞扫描设备

参数性质	序号	具体技术(参数)要求
------	----	------------

	1	<p>1.性能参数：要求设备系统漏扫授权IP数≥100，WEB漏扫授权URL数≥20；性能指标：主机漏扫最大并发IP数≥75，WEB漏扫最大并发URL数≥5。硬件参数：内存大小≥8G，接口≥6千兆电口+2千兆光口SFP。</p> <p>2.支持同时开启全插件系统漏洞扫描、WEB漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h；</p> <p>3.支持从“高危”、“中危”、“低危”、“信息”四个安全级别展示漏洞风险等级的分布情况；</p> <p>4.支持多种系统漏洞检测技术，如：基于漏洞原理的原理扫描技术、基于banner信息的漏洞扫描技术等。</p> <p>5.风险统计方面，支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情；</p> <p>6.支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情；</p> <p>7.支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入；</p> <p>8.资产发现支持并发扫描数量自定义，最大并发扫描IP数为1024；</p> <p>9.在报告管理方面，产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表；</p> <p>10.支持操作系统、网络设备、数据库、中间件等漏洞扫描；</p> <p>11.支持多种系统漏洞检测技术，如：基于漏洞原理的原理扫描技术、基于banner信息的漏洞扫描技术等；</p> <p>12.支持快速扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中快速扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。</p> <p>13.支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入。</p> <p>14.支持报表比对功能，可对任意两次同类型的报表进行比对，输出比对报表，并支持以EXCEL格式导出。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。	

附表四：其他计算机设备及软件

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1. 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，终端客户端软件包含100台PC客户端授权和10台服务器旗舰版授权。</p> <p>2. 采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能；</p> <p>3. 支持显示当前未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量；</p> <p>4. 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议。</p> <p>5. 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；</p> <p>6. 支持按“最近 7 天”、“最近 30 天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒 TOP5 排行榜，并展示对应的事件数及终端数；</p> <p>7. 支持展示全球热点风险事件在网内终端的爆发情况，及时了解、处置网内终端的热点风险事件，并显示影响终端数量；</p> <p>8.支持全网终端资产清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。</p> <p>9.支持对安装了指定版本操作系统、特定应用软件、开放了高危端口的风险主机进行统计，具备对风险主机进行漏洞扫描、安装高危软件的主机列表信息统计导出、高危端口一键封堵的能力。</p> <p>10.提供对业务系统之间、业务系统内不同应用角色或主机之间、业务系统内相同应用角色之间的访问控制策略配置，并可以图形化显示业务系统、主机及流量详情。</p> <p>11支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4 地址、MAC地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新；</p> <p>12. 具备主机发现的能力，管理员可以按照扫描网段、扫描方式、扫描协议、扫描端口对主机进行扫描，来及时发现尚未管控的主机资产，并将所发现的主机列表导出；</p> <p>13.支持实时监控诱饵文件，能够在勒索病毒修改或加密文件时对该操作进行拦截。</p> <p>14.支持根据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志的查询和检测；</p> <p>15.支持针对管理控制中心性能，安全事件，勒索病毒事件等邮件告警；</p> <p>16.一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、恶意代码防范、访问控制、安全审计、访问控制、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。</p> <p>17.支持终端管理功能，可以灵活的部署和配置安全策略，支持安全策略模板和安全策略一体化配置，其中安全策略模板可以对指定终端组快速部署安全策略。</p> <p>18.支持主机分组，并支持主机防病毒系统软件版本的错峰和灰度升级，可以根据云平台实际情况控制云主机同时升级的最大数量，避免大量云主机防病毒软件同时更新造成网络拥堵或 I/O 风暴，并支持主机防病毒软件的启用禁用和重启，在管理平台中心可以直接卸载主机软件。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表五：综合日志审计

参数性质	序号	具体技术(参数)要求
------	----	------------

	<p>1.性能参数：要求默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥1TB，平均每秒处理日志数≥1200。2U设备，内存至少为8G，至少提供6个千兆电口和日志分析系统软件一套；</p> <p>2.支持自定义首页卡片，支持实时监控日志传输量和日志留存的合规情况。</p> <p>3.支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等</p> <p>4.支持以列表的方式展示告警：告警声音设置：告警过滤策略</p> <p>5.支持全文检索功能，能对系统内的对象提供全文检索功能</p> <p>6.支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。</p> <p>7.支持内置实例管理和报表任务管理</p> <p>8.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。</p> <p>9.支持定义部门和人员的对应关系；支持定义人员与账号的对应关系；</p> <p>10.可通过自定义聚合规则修改日志的聚合归并逻辑规则，提高日志分析效率，支持归并技术，一段时间内对重复日志进行归并；</p> <p>11.支持自定义仪表盘，客户可以选择对应的微件，组成想要关注的仪表展现内容；</p> <p>12.支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；</p> <p>13.支持业务管理配置，可以导出系统内报表、策略、采集器、资产等业务数据，供新设备导入配置，实现快速切换设备</p> <p>14.支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现</p> <p>15.支持集群配置及集群状态监控</p> <p>16.支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用</p> <p>17.支持多种方式的查询检索，包括：日志检索、资产检索、告警检索、事件检索；</p> <p>18.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表六：堡垒机

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1.性能参数：要求提供运维授权数≥50个，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200。硬件参数：内存大小≥4G，硬盘容量≥1T SATA，接口≥6千兆电口。包含安全运维管理软件一套；</p> <p>2. 支持RDP协议的控制台登录控制；</p> <p>3. 支持按加密格式导入、导出运维授权数据，方便授权关系备份以及授权数据迁移；</p> <p>4. 支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问；</p> <p>5. 支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批。</p> <p>6. 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯；</p> <p>7. 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；</p> <p>8. 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。</p> <p>9. 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯。</p> <p>10.支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人；</p> <p>11. 为适应信息化发展趋势，要求全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计；</p> <p>12. 图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放；</p> <p>13. 支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；</p> <p>14. 支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表七：网络准入

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1.网络层吞吐量≥2Gb，应用层吞吐量≥150Mb，支持用户数≥500，准入终端数≥250，每秒新建连接数≥1000，最大并发连接数≥50000。接口≥4千兆电口。</p> <p>2. 支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能，支持旁路模式，无需更改网络配置，实现上网行为审计及准入控制功能。</p> <p>3. 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；</p> <p>4. 支持DNS透明代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至制定线路；</p> <p>5. 支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等。</p> <p>6. 支持在不安装客户端的状态下，通过流量状况检查10款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复。</p> <p>7. 支持首页分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况。</p> <p>8. 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等。</p> <p>9. 同一个账号，支持与指定数量的多个终端进行自动绑定，支持多人使用同一帐号登录，且支持重复登陆检测机制，限制公共账号的使用人数。</p> <p>10. 支持LDAP、Radius、POP3、Proxy等第三方认证；支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证。</p> <p>11. 支持Web访问质量检测，可针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，可以列表形式展示访问质量差的用户名单并对单用户进行定向web访问质量检测。</p> <p>12. 认证成功用户支持页面跳转：1. 跳转到用户原本输入的URL地址；2.跳转到管理员指定的URL地址；3. 跳转到注销页面；</p> <p>13. 能够与本项目中防毒墙产品实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；</p> <p>14. 支持终端用户可以使用账号绑定的手机号码，接收短信验证码，然后使用手机号码和验证码完成密码认证；支持在终端用户的账号存在微信绑定关系的情况下，PC端的终端用户可以直接使用微信扫码二维码完成密码认证过程，移动端的终端用户，可以直接打开微信扫码完成密码认证过程。</p> <p>15. 为保证应用识别的准确率，设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6500种以上的应用，并保持每两个星期更新一次；</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表八：终端安全管理

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1.此次配置终端安全管理软件支持100点终端管理</p> <p>2.所有功能的导入只需要在终端上安装一个客户端，即可实现所有的功能，确保终端具有良好的兼容性</p> <p>3.所有功能的管理均通过同一个控制台进行统一管理</p> <p>4.本系统的服务器端数据库需搭建在MSsql或者MySQL上</p> <p>5.可通过应用程序、端口、网络地址、通讯方向等参数限制计算机的网络访问权限，可限制单向或双向的通讯方向</p> <p>6.可自定义网络地址和网络端口类别，方便归类管理</p> <p>7.可检测内部网络是否有外来计算机非法接入并提供实时报警</p> <p>8.可与安全检测功能相结合，阻断不合规客户端访问网络，直到终端符合安全检测的要求，才允许访问网络</p> <p>9.可按“时间”、“到期时间”、“仅离线生效”灵活设置策略</p> <p>10.当终端的通讯行为触发策略时，支持记录下当时的屏幕画面或锁定计算机</p> <p>11.可按时间、计算机范围、网络地址（明细、类别）、端口（明细、类别）、流量方向（发送、接收、合计）等方式对网络流量进行统计，并可自定义TOP显示</p> <p>12.统计结果至少支持列表和图表（柱状图、饼状图）两种显示方式</p> <p>13.可根据网络地址、端口、流量方向等参数限制计算机的网络流量，达到合理分配带宽的目的</p> <p>14.可自定义网络地址类别和网络端口类别，方便归类管理</p> <p>15.支持远程查看客户端计算机当前运行的应用程序、进程、性能、设备管理、系统服务、磁盘管理、共享文件夹、计划任务、用户和组、启动项等，并可对应用程序、进程、系统服务、共享文件夹等进行操作，如可关闭当前运行的应用程序、进程等</p> <p>16.支持远程卸载客户端计算机安装的软件，并支持对安装项信息进行自定义卸载</p> <p>17.可点对多远程连接到远端计算机的桌面，直接对计算机进行操作，并支持对远端计算机的键盘、鼠标进行控制</p> <p>18.支持对客户端下达任务，将客户端全盘文件目录列表或U盘文件列表上传到服务器，支持把客户端某个指定的文件上传到服务器</p> <p>19.可点对多远程连接到远端计算机的桌面，直接对计算机进行操作，并支持对远端计算机的键盘、鼠标进行控制</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

第三章 供应商须知

一、前附表：

序号	条款名称	内容及要求
1	计划编号	克东财购核字[2021]00023号
2	项目编号	[230230]KDC[TP]20210009
3	项目名称	网络等级保护二级设备
4	包组情况	共1包
5	采购资金预算金额	718,000.00
6	采购方式	竞争性谈判
7	开标方式	不见面开标

8	评标方式	现场网上评标
9	评标办法	合同包1（网络等级保护二级设备）：最低评标价法
10	现场踏勘	是
11	保证金缴纳截止时间（同递交响应文件截止时间）	详见采购公告
12	电子响应文件递交	电子响应文件在响应截止时间前递交至黑龙江省项目采购电子交易系统
13	响应有效期	从提交投标（响应）文件的截止之日起90日历天
14	响应文件要求	<p>（1）加密的电子响应文件 1 份（需在投标截止时间前上传至“黑龙江省项目采购电子交易系统”）。</p> <p>（2）为避免上传的电子投标文件出现无法使用的情况，若项目采用现场开标方式时，投标人需自行携带投标客户端生成的备用电子标投标文件（.备用文件）U盘（或光盘）{{非加密电子版响应文件数}}份；若项目采用远程开标方式时，在代理机构开启备用文件上传功能后，投标人需自行上传备用电子标投标文件（.备用文件）。</p> <p>（3）纸质响应文件正本 {{纸质响应文件正本}} 份，纸质响应文件副本 {{纸质响应文件副本}} 份。</p>
15	中标候选人推荐家数	合同包1（网络等级保护二级设备）： 3
16	中标供应商确定	采购人授权谈判小组按照评审原则直接确定中标（成交）人。
17	备选方案	不允许
18	联合体投标	包1： 不接受
19	代理服务费	无
20	代理服务费收取方式	不收取。 不收取
21	投标保证金	<p>本项目允许投标供应商按照相关法律法规自主选择以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式缴纳保证金。</p> <p>网络等级保护二级设备：保证金人民币：0.00元整。</p> <p>开户单位： 无</p> <p>开户银行： 无</p> <p>银行账号： 无</p> <p>特别提示：</p> <p>1、响应供应商应认真核对账户信息，将响应保证金足额汇入以上账户，并自行承担因汇错投标保证金而产生的一切后果。响应保证金到账（保函提交）的截止时间与响应截止时间一致，逾期不交者，响应文件将作无效处理。</p> <p>2、响应供应商在转账或电汇的凭证上应按照以下格式注明，以便核对：“（项目编号：***、包组：***）的响应保证金”。</p>

22	电子招投标	<p>各响应供应商须在响应截止时间前上传加密的电子响应文件至“黑龙江省项目采购电子交易系统”。且需携带响应单位有效CA前往开标现场。各响应供应商未在响应截止时间前上传电子响应文件的，视为自动放弃响应。响应供应商所编制的电子响应文件、开标时递交的U盘（或光盘）存储的非加密响应文件内容应一致。投标供应商因系统或网络问题无法上传电子响应文件时，请在工作时间及时拨打联系电话：4009985566按5转1。</p> <p>1、本项目采用电子开标（网上开标），如在开标过程中出现意外情况导致无法继续进行电子开标时，改为非加密电子响应文件开标。本项目采用电子评标（网上评标），只对加密电子响应文件进行评审，如在评标过程中出现意外情况导致无法继续进行电子评标时，改为非加密电子响应文件评标。</p> <p>2、定义：</p> <p>（1）电子响应文件是指通过投标客户端编制，在电子响应文件中，涉及“加盖单位公章”的内容应使用单位电子公章完成加密后，成功上传至黑龙江省项目采购电子交易系统的最终版指定格式电子响应文件；</p> <p>（2）非加密电子版响应文件是指存储在U盘（或光盘）中的响应文件。</p> <p>3、使用投标客户端，经过编制、签章，在生成加密响应文件时，会同时生成非加密响应文件，供响应供应商刻录使用。U盘（或光盘）由响应供应商自行刻录、存储，响应供应商必须保证电子存储设备能够正常读取。U盘（或光盘）表面、外包装上应简要载明项目编号、项目名称、响应单位名称等信息。</p> <p>4、响应供应商的法定代表人或其委托代理人应当按照本招标公告载明的时间和地点参加开标。开标时，响应供应商应当使用CA在采购代理机构设置的时间内完成响应文件在线解密。</p> <p>5、开标时出现下列情况的，采购人、采购代理机构视其为无效投标：</p> <p>（1）经检查数字证书无效的响应文件；</p> <p>（2）投标供应商应在采购代理机构设置的时间内完成解密，因自身原因造成电子响应文件未能解密的；</p> <p>（3）开标现场无法使用系统进行电子开评标时，响应供应商未按招标文件要求提供非加密电子响应文件的；</p> <p>（4）逾期送达或者未按照招标文件要求密封的响应文件。</p> <p>6、本招标项目的响应供应商必须在开标时间开始后完成所投全部包组的电子响应文件在线解密。投标供应商必须保证在采购代理机构设置的时间内完成全部包组的电子响应文件解密。</p>
23	电子响应文件签字、盖章要求	<p>应按照第六章“响应文件格式与要求”，使用CA进行签字、盖章。</p> <p>说明：若涉及到授权委托人签字的可将文件签字页先进行签字、扫描后导入加密电子响应文件或签字处使用电脑打字输入。</p>
24	其他	
25	项目兼投兼中规则	兼投兼中：本项目兼投兼中。

二.响应须知

1.响应方式

1.1 响应方式采用网上响应，流程如下：

供应商应在黑龙江省政府采购网（<http://hljcg.hlj.gov.cn>）提前注册并办理电子签章CA，CA用于制作响应文件时盖章、加密和开标时解密（CA办理流程及驱动下载参考黑龙江省政府采购网（<http://hljcg.hlj.gov.cn>）办事指南-CA办理流程）具体操作步骤，在黑龙江省政府采购网（<http://hljcg.hlj.gov.cn/>）下载政府采购供应商操作手册。

1.2缴纳保证金（如有）。本采购项目采用“虚拟子账号”形式收退保证金，每一个供应商在所投的每一项目下合同包会对应每一家银行自动生成一个账号，称为“虚拟子账号”。在进行响应信息确认后，应通过应标管理-已响应的项目，选择缴纳银行并获取对应不同包的缴纳金额以及虚拟子账号信息，并在开标时间前，通过转账至上述账号中，付款人名称必须为响应单位全称且与响应信息一致。

若出现账号缴纳不一致、缴纳金额与供应商须知前附表规定的金额不一致或缴纳时间超过开标时间，将导致保证金缴纳失败。

1.3查看响应状况。通过应标管理-已响应的项目可查看已响应项目信息。

2.特别提示：

2.1 由于保证金到账需要一定时间，请供应商在递交响应文件截止前及早缴纳。

三.说明

1.总则

1.1本谈判文件依据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和《政府采购非招标采购方式管理办法》（财政部令第74号）及国家和黑龙江省有关法律、法规、规章制度编制。

1.2供应商应仔细阅读本项目信息公告及谈判文件的所有内容（包括变更、补充、澄清以及修改等，且均为谈判文件的组成部分），按照谈判文件要求以及格式编制响应文件，并保证其真实性，否则一切后果自负。

1.3本次公开采购项目，是以谈判公告的方式邀请非特定的供应商参加响应。

2.适用范围

2.1本谈判文件仅适用于本次谈判公告中所涉及的项目和内容。

3.响应费用

3.1供应商应承担所有与准备和参加响应有关的费用。不论响应结果如何，采购代理机构和采购人均无义务和责任承担相关费用。

4.当事人

4.1“采购人”是指依法进行政府采购的国家机关、事业单位、团体组织。本谈判文件的采购人特指克东县财政局。

4.2“采购代理机构”是指本次采购项目活动组织方。本谈判文件的采购代理机构特指克东县公共资源交易综合服务中心。

4.3“供应商”是指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

4.4“谈判小组”是指根据《中华人民共和国政府采购法》等法律法规规定，由采购人代表和有关专家组成以确定成交供应商或者推荐成交候选人的临时组织。

4.5“成交人”是指经谈判小组评审确定的对谈判文件做出实质性响应，取得与采购人签订合同资格的供应商。

5.合格的供应商

5.1 符合本谈判文件规定的资格要求，并按照规定提供相关证明材料。

5.2 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

5.3 为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

6.以联合体形式响应的，应符合以下规定

6.1 联合体各方应签订联合体协议书，明确联合体牵头人和各方权利义务，并作为响应文件组成部分。

6.2 联合体各方均应当具备政府采购法第二十二条规定的条件，并在响应文件中提供联合体各方的相关证明材料。

6.3 联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

6.4 联合体各方中至少应当有一方符合采购人规定的资格要求。由同一资质条件的供应商组成的联合体，应当按照资质等级较低的供应商确定联合体资质等级。

6.5 联合体各方不得再以自己名义单独在同一项目中响应，也不得组成新的联合体参加同一项目响应。

6.6 联合体各方应当共同与采购人签订采购合同，就合同约定的事项对采购人承担连带责任。

6.7 响应时，应以联合体协议中确定的主体方名义响应，以主体方名义缴纳保证金，对联合体各方均具有约束力。

7.语言文字以及度量衡单位

7.1 所有文件使用的语言文字为简体中文。专用术语使用外文的，应附有简体中文注释，否则视为无效。

7.2 所有计量均采用中国法定的计量单位。

7.3 所有报价一律使用人民币，货币单位：元。

8. 现场踏勘

8.1 谈判文件规定组织踏勘现场的，采购人按谈判文件规定的时间、地点组织供应商踏勘项目现场。

8.2 供应商自行承担踏勘现场发生的责任、风险和自身费用。

8.3 采购人在踏勘现场中介绍的资料和数据，不构成对谈判文件的修改或不作为供应商编制响应文件的依据。

9.其他条款

无论成交与否供应商递交的响应文件均不予退还。

四.谈判文件的澄清或者修改

采购人或采购代理机构需对谈判文件作实质性变动的，应当在规定的截止时间前3个工作日以公告形式告知所有参加谈判的供应商，不足3个工作日的，顺延提交首次响应文件截止之日，同时在“黑龙江省政府采购网”上发布澄清或者变更公告。澄清或者变更公告的内容为谈判文件的组成部分，供应商应自行上网查询，采购人或采购代理机构不承担供应商未及时关注相关信息的责任。

五、响应文件

1.响应文件的构成

响应文件应按照谈判文件第七章“响应文件格式”进行编写（可以增加附页），作为响应文件的组成部分。

2.响应报价

2.1 供应商应按照“第四章采购内容及要求”的需求内容、责任范围以及合同条款进行报价。并按“首轮报价表”和“分项报价明细表”规定的格式报出总价和分项价格。响应总价中不得包含谈判文件要求以外的内容，否则，在评审时不予核减。

2.2 响应报价包括本项目采购需求和投入使用的所有费用，如主件、标准附件、备品备件、施工、服务、专用工具、安装、调试、检验、培训、运输、保险、税款等。

2.3 响应报价不得有选择性报价和附有条件的报价。

2.4 对报价的计算错误按以下原则修正：

（1）响应文件中首轮报价表（报价表）内容与响应文件中相应内容不一致的，以首轮报价表（报价表）为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

(3) 单价金额小数点或者百分比有明显错位的，以首轮报价表的总价为准，并修改单价。

注：修正后的报价供应商应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字确认后产生约束力，但不得超出响应文件的范围或者改变响应文件的实质性内容，供应商不确认的，其响应无效。

3. 投标有效期

3.1 投标有效期从提交响应文件的截止之日起算。响应文件中承诺的投标有效期应当不少于谈判文件中载明的投标有效期。投标有效期内供应商撤销响应文件的，采购人或者采购代理机构可以不退还保证金。

3.2 出现特殊情况需要延长投标有效期的，采购人以书面形式通知所有供应商延长投标有效期。供应商同意延长的，应相应延长其保证金的有效期，但不得要求或被允许修改或撤销其响应文件；供应商拒绝延长的，其响应失效，但供应商有权收回其保证金。

4. 保证金

4.1 保证金的缴纳

供应商在提交响应文件的同时，应按供应商须知前附表规定的金额、开户银行、行号、开户单位、账号和谈判文件本章“响应须知”规定的保证金缴纳要求递交保证金，并作为其响应文件的组成部分。

4.2 保证金的退还：

(1) 供应商在递交截止时间前放弃响应的，自所投合同包结果公告发出后5个工作日内退还，但因供应商自身原因导致无法及时退还的除外；

(2) 未成交人保证金，自成交通知书发出之日起5个工作日内退还；

(3) 成交人保证金，自政府采购合同签订之日起5个工作日内退还。

4.3 有下列情形之一的，保证金将不予退还：

(1) 成交后，无正当理由放弃中标资格；

(2) 成交后，无正当理由不与采购人签订合同；

(3) 在签订合同时，向采购人提出附加条件；

(4) 不按照谈判文件要求提交履约保证金；

(5) 要求修改、补充和撤销响应文件的实质性内容；

(6) 要求更改谈判文件和成交结果公告的实质性内容；

(7) 法律法规和谈判文件规定的其他情形。

5. 响应文件的修改和撤回

5.1 供应商在提交递交截止时间前，可以对所递交的响应文件进行补充、修改或者撤回。补充、修改的内容旁签署（法人或授权委托人签署）、盖章、密封和上传至系统后生效，并作为响应文件的组成部分。

5.2 在提交响应文件截止时间后到谈判文件规定的投标有效期终止之前，供应商不得补充、修改、替代或者撤回其响应文件。

6. 响应文件的递交

6.1 在谈判文件要求提交响应文件的截止时间之后送达的响应文件或上传的响应文件，为无效响应文件，采购单位或采购代理机构拒收。采购人、采购代理机构对误投或未按规定时间、地点或模式进行响应的概不负责。

7. 样品（演示）

7.1 谈判文件规定供应商提交样品的，样品属于响应文件的组成部分。样品的生产、运输、安装、保全等一切费用由供应商自理。

7.2 开标前，供应商应将样品送达至指定地点，并按要求摆放并做好展示。若需要现场演示的，供应商应提前做好演示准备（包括演示设备）。

7.3评标结束后，成交人与采购人共同清点、检查和密封样品，由成交人送至采购人指定地点封存。未成交供应商将样品自行带回。

六.开标、评审、结果公告、成交通知书发放

1.开标程序

1.1主持人按下列程序进行开标：

- (1) 宣布开标纪律；
- (2) 宣布开标会议相关人员姓名；
- (3) 供应商对已提交的加密文件进行解密，由采购人或者采购代理机构工作人员当众宣布供应商名称；
- (4) 开标结束，响应文件移交谈判小组。

1.2开标异议

供应商代表对开标过程和开标记录有疑义，以及认为采购人、采购代理机构相关工作人员有需要回避的情形的，应当当场提出询问或者回避申请，开标会议结束后不再接受相关询问、质疑或者回避申请。

1.3备注说明：

1.3.1若本项目采用不见面开标，开标时供应商使用 CA证书参与远程响应文件解密。供应商用于解密的 CA证书应为该响应文件生成加密、上传的同一把 CA证书。/p>

1.3.2若本项目采用不见面开标，供应商在开标时间前30分钟，应当提前登录开标系统进行签到，填写联系人姓名与联系号码；在系统约定时间内使用 CA证书签到以及解密，未成功签到或未成功解密的视为其无效响应。

1.3.3供应商对不见面开标过程和开标记录有疑义，应在开标系统规定时间内在不见面开标室提出异议，采购代理机构在网上开标系统中进行查看及回复。开标会议结束后不再接受相关询问、质疑或者回避申请。

2.评审（详见第六章）

3.结果公告

3.1成交供应商确定后，采购代理机构将在黑龙江省政府采购网、黑龙江省公共资源交易网上发布成交结果公告，同时将成交结果以公告形式通知未成交的供应商，成交结果公告期为 1 个工作日。

3.2项目废标后，采购代理机构将在黑龙江省政府采购网、黑龙江省公共资源交易网上发布废标公告，废标结果公告期为 1 个工作日。

4.成交通知书发放

4.1发布成交结果的同时，成交供应商可自行登录黑龙江省政府采购网--政府采购云平台打印成交通知书，成交通知书是合同的组成部分，成交通知书对采购人和成交供应商具有同等法律效力。

4.2成交通知书发出后，采购人不得违法改变成交结果，成交人无正当理由不得放弃成交。

七.询问、质疑与投诉

1.询问

1.1 供应商对政府采购活动事项有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构应当在3个工作日内做出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知其向采购人提出。

1.2为了使提出的询问事项在规定时间内得到有效回复，询问采用实名制，询问内容以书面材料的形式亲自递交到采购代理机构，正式受理后方可生效，否则，为无效询问。

2.质疑

2.1供应商认为采购文件、采购过程和成交、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之

日起七个工作日内，以书面形式向采购人或采购代理机构提出质疑。

供应商在法定质疑期内应当一次性提出针对同一采购程序环节的质疑。

提出质疑的供应商应当是参与所质疑项目采购活动的供应商。

潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。对采购文件提出质疑的，应当在获取采购文件或者采购文件公告期限届满之日起7个工作日内提出。

2.2采购人应当在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复的内容不得涉及商业秘密。

2.3询问或者质疑事项可能影响成交结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

2.4供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

- (一) 供应商的姓名或者名称、地址、邮编、联系人及联系电话；
- (二) 质疑项目的名称、编号；
- (三) 具体、明确的质疑事项和与质疑事项相关的请求；
- (四) 事实依据；
- (五) 必要的法律依据；
- (六) 提出质疑的日期。

注：对谈判文件质疑的，还需提供供应商首次下载采购文件的时间截图。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

供应商可以授权代表进行质疑，且应当提交供应商签署的授权委托书。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

2.5供应商在提出质疑时，请严格按照相关法律法规及质疑函范本要求提出和制作，否则，自行承担相关不利后果。

对捏造事实，提供虚假材料或者以非法手段取得证明材料进行恶意质疑的，一经查实，将上报监督部门，并给以相应处罚。

2.6接收质疑函的方式：为了使提出的质疑事项在规定时间内得到有效答复、处理，质疑采用实名制，且由法定代表人或授权代表亲自递交至采购人或采购代理机构，正式受理后方可生效。

联系部门：采购人、采购代理机构（详见第一章 响应邀请）。

联系电话：采购人、采购代理机构（详见第一章 响应邀请）。

通讯地址：采购人、采购代理机构（详见第一章 响应邀请）。

3.投诉

质疑人对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内做出书面答复的，可以在答复期满后十五个工作日内向监督部门进行投诉。投诉程序按《政府采购法》及相关规定执行。

供应商投诉的事项不得超出已质疑事项的范围。

第三章 合同与验收

一.合同要求

1.一般要求

1.1采购人应当自成交通知书发出之日起30日内，按照谈判文件和成交人响应文件的规定，与成交人签订书面合同。所签订的合同不得对谈判文件确定的事项和成交人响应文件作实质性修改。

合同签订双方不得提出任何不合理的要求作为签订合同的条件。

1.2 政府采购合同应当包括采购人与中标人的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

1.3 采购人与成交人应当根据合同的约定依法履行合同义务。

政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。

政府采购合同的双方当事人不得擅自变更、中止或者终止合同。

1.4 拒绝签订采购合同的按照相关规定处理，并承担相应法律责任。

1.5 采购人应当自政府采购合同签订之日起2个工作日内，将政府采购合同在省级以上人民政府财政部门指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

2. 合同格式及内容

2.1 具体格式见本谈判文件后附拟签订的《合同文本》（部分合同条款），响应文件中可以不提供《合同文本》。

2.2 《合同文本》的内容可以根据《民法典》和合同签订双方的实际要求进行修改，但不得改变范本中的实质性内容。

二.验收

成交人在供货、工程竣工或服务结束后，采购人应及时组织验收，并按照谈判文件、响应文件及合同约定填写验收单。

政府采购合同（合同文本）

甲方：***（填写采购单位）

地址（详细地址）：

乙方：***（填写中标供应商）

地址（详细地址）：

合同号：

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等相关法律法规，甲、乙双方就（填写项目名称）（政府采购项目编号、备案编号：），经平等自愿协商一致达成合同如下：

1. 合同文件

本合同所附下列文件是构成本合同不可分割的部分：

(1) 合同格式以及合同条款

(2) 中标结果公告及中标通知书

(3) 谈判文件

(4) 响应文件

(5) 变更合同

2. 本合同所提供的标的物、数量及规格等详见中标结果公告及后附清单。

3. 合同金额

合同金额为人民币 万元，大写：

4. 付款方式及时间

***（见谈判文件第四章）

5. 交货安装

交货时间：

交货地点：

6. 质量

乙方提供的标的物应符合国家相关质量验收标准，且能够提供相关权威部门出具的产品质量检测报告；提供的相关服务符合国家（或行业）规定标准。

7. 包装

标的物的包装应按照国家或者行业主管部门的技术规定执行，国家或业务主管部门无技术规定的，应当按双方约定采取足以保护标的物安全、完好的包装方式。

8.运输要求

- (1) 运输方式及线路:
- (2) 运输及相关费用由乙方承担。

9.知识产权

乙方应保证甲方在中国境内使用标的物或标的物的任何一部分时，免受第三方提出的侵犯其知识产权的诉讼。

10.验收

- (1) 乙方将标的物送达至甲方指定的地点后，由甲乙双方及第三方（如有）一同验收并签字确认。
- (2) 对标的物的质量问题，甲方应在发现后向乙方提出书面异议，乙方在接到书面异议后，应当在 日内负责处理。甲方逾期提出的，对所交标的物视为符合合同的规定。如果乙方在响应文件及谈判过程中做出的书面说明及承诺中，有明确质量保证期的，适用质量保证期。
- (3) 经双方共同验收，标的物达不到质量或规格要求的，甲方可以拒收，并可解除合同且不承担任何法律责任，

11.售后服务

- (1) 乙方应按谈判文件、响应文件及乙方在谈判过程中做出的书面说明或承诺提供及时、快速、优质的售后服务。
- (2) 其他售后服务内容： （响应文件售后承诺等）

12.违约条款

- (1) 乙方逾期交付标的物、甲方逾期付款，按日承担违约部分合同金额的违约金。
- (2) 其他违约责任以相关法律法规规定为准，无相关规定的，双方协商解决。

13.不可抗力条款

因不可抗力致使一方不能及时或完全履行合同的，应及时通知另一方，双方互不承担责任，并在 天内提供有关不可抗力相关证明。合同未履行部分是否继续履行、如何履行等问题，双方协商解决。

14.争议的解决方式

合同发生纠纷时，双方应协商解决，协商不成可以采用下列方式解决：

- (1) 提交 仲裁委员会仲裁。
- (2) 向 人民法院起诉。

15.合同保存

合同文本一式五份，采购单位、供应商、政府采购监管部门、采购代理机构、国库支付执行机构各一份，自双方签订之日起生效。

16.合同未尽事宜，双方另行签订补充协议，补充协议是合同的组成部分。

甲方： （章） 乙方： （章）
采购方法人代表： （签字） 供应商法人代表： （签字）
开户银行： 开户银行：
帐号： 帐号：
联系电话： 联系电话：

签订时间 年 月 日

附表：标的物清单（主要技术指标需与响应文件相一致）（工程类的附工程量清单等）

名称	品牌、规格、标准/主要服务内容	产地	数量	单位	单价（元）	金额（元）
**	**	**	**	**	**	**

名称	品牌、规格、标准/主要内容	产地	数量	单位	单价（元）	金额（元）
合计：人民币大写：**元整						¥：**

第四章 谈判内容与技术要求

一、项目概况：

本项目是按照《黑龙江省财政厅关于做好全省财政专网网络安全等级保护工作的通知》（黑财函【2021】202号）的要求，加强全省财政网络安全工作，保障预算管理二级等保系统安全稳定运行，特别是确保财政支付电子化安全管理，按照省厅提供的标准要求，我县需采购网络等级保护二级设备及2台防毒墙，加强网络安全运营。

合同包1（网络等级保护二级设备）

1.主要商务要求

标的提供的时间	合同签订后30个日历日内交货
标的提供的地点	黑龙江省齐齐哈尔市克东县财政局圣水路18号
投标有效期	从提交投标（响应）文件的截止之日起90日历天
付款方式	1期：支付比例100%，项目验收合格后一次性付清
验收要求	1期：符合《黑龙江省财政厅关于做好全省财政专网网络安全等级保护工作的通知》中二级等保要求
履约保证金	不收取
其他	现场踏勘时间、地点、售后、质保期、联系人、联系方式：1、踏勘时间1月30日 2、地点克东县财政局 3、联系人郭朗、联系电话18945211201 4、质量保证自安装日起至2023年1月，期间出现质量问题应及时更换或维修 5、售后服务自安装日起至2023年1月，如有技术操作及时远程操作或电话指挥操作 6、提供自安装日起至2026年1月期间所有软件更新升级服务。

2.技术标准与要求

序号	核心产品 （“△”）	品目名称	标的名称	单位	数量	分项预算单 价（元）	分项预算总 价（元）	面向对 象情况	所属 行业	招标技 术要求
1		其他交换设备	其他交换设备	台	200	63,000.00	126,000.00	否	-	详见附件一
2		入侵防御设备	入侵防御设备	台	100	50,000.00	50,000.00	否	-	详见附件二
3		漏洞扫描设备	漏洞扫描设备	台	100	150,000.00	150,000.00	否	-	详见附件三
4		其他计算机设备及软件	其他计算机设备及软件	套	100	38,000.00	38,000.00	否	-	详见附件四
5		其他交换设备	综合日志审计	台	100	113,000.00	113,000.00	否	-	详见附件五

序号	核心产品 ("△")	品目名称	标的名称	单位	数量	分项预算单 价(元)	分项预算总 价(元)	面向对 象情况	所属 行业	招标技 术要求
6		其他交换设备	堡垒机	台	1. 0 0	110,000.00	110,000.00	否	-	详见附 表六
7		其他交换设备	网络准入	台	1. 0 0	63,000.00	63,000.00	否	-	详见附 表七
8		服务器	终端安全管理	套	1. 0 0	68,000.00	68,000.00	否	-	详见附 表八

附表一：其他交换设备

参数性质	序 号	具体技术(参数)要求

1	<p>1、设备支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>2、设备具备链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。</p> <p>3、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。</p> <p>4、设备具备与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理。</p> <p>5、设备具备安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。</p> <p>6、设备具备策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。。</p> <p>7、设备具备多种自定义条件快速查询安全日志，自定义条件至少包括时间、日志类型、安全日志严重等级等条件。</p> <p>8、设备具备三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色。</p> <p>9、网络层吞吐量≥3G，应用层吞吐量≥600M;IPS吞吐量≥150M，防病毒吞吐量≥250M，并发连接数≥80万，HTTP新建连接数≥1.8万。接口：≥6千兆电口。</p> <p>10、设备具备不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>11、设备具备多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。</p> <p>12、设备具备全面的URL分类库，针对网站类别实现细粒度管控，杜绝非法、违规网站的访问行为。</p> <p>13、设备具备对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。</p> <p>14、设备具备对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置。</p> <p>15、设备具备病毒例外特征设置，根据文件MD5值和文件URL设置病毒白名单，不对白名单进行病毒查杀。</p> <p>16、设备具备勒索病毒检测与防御功能。</p> <p>17、设备支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。</p> <p>18、设备支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表二：入侵防御设备

参数性质	序号	具体技术(参数)要求
------	----	------------

	1	<p>1.产品支持NAT64和NAT46 地址转换方式，满足IPv6改造要求。</p> <p>2.产品支持多种用户认证方式，用户认证方式要求支持本地密码认证、外部密码认证和单点登陆等方式。</p> <p>3.产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能。</p> <p>4.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。</p> <p>5.产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。</p> <p>6.产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。</p> <p>7.网络层吞吐量≥3G，应用层吞吐量≥600M，并发连接数≥80万，HTTP新建连接数≥1.8万。1U机架式设备，单电源，接口≥6千兆电口。需具备web层应用防护能力。</p> <p>8.产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。</p> <p>9.产品支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。</p> <p>10.产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。当主机进行合法外联时，支持对不少于9800种应用的识别和控制。应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。</p> <p>11.产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。</p> <p>12.支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。</p> <p>13.支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。	

附表三：漏洞扫描设备

参数性质	序号	具体技术(参数)要求
------	----	------------

	1	<p>1.性能参数：要求设备系统漏扫授权IP数≥100，WEB漏扫授权URL数≥20；性能指标：主机漏扫最大并发IP数≥75，WEB漏扫最大并发URL数≥5。硬件参数：内存大小≥8G，接口≥6千兆电口+2千兆光口SFP。</p> <p>2.支持同时开启全插件系统漏洞扫描、WEB漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h；</p> <p>3.支持从“高危”、“中危”、“低危”、“信息”四个安全级别展示漏洞风险等级的分布情况；</p> <p>4.支持多种系统漏洞检测技术，如：基于漏洞原理的原理扫描技术、基于banner信息的漏洞扫描技术等。</p> <p>5.风险统计方面，支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情；</p> <p>6.支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情；</p> <p>7.支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入；</p> <p>8.资产发现支持并发扫描数量自定义，最大并发扫描IP数为1024；</p> <p>9.在报告管理方面，产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表；</p> <p>10.支持操作系统、网络设备、数据库、中间件等漏洞扫描；</p> <p>11.支持多种系统漏洞检测技术，如：基于漏洞原理的原理扫描技术、基于banner信息的漏洞扫描技术等；</p> <p>12.支持快速扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中快速扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。</p> <p>13.支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入。</p> <p>14.支持报表比对功能，可对任意两次同类型的报表进行比对，输出比对报表，并支持以EXCEL格式导出。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。	

附表四：其他计算机设备及软件

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<ol style="list-style-type: none"> 1. 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，终端客户端软件包含100台PC客户端授权和10台服务器旗舰版授权。 2. 采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能； 3. 支持显示当前未处理的勒索病毒数量、暴力破解数量、僵尸网络、WebShell后门数量、高危漏洞及其各自影响的终端数量； 4. 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议。 5. 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数； 6. 支持按“最近 7 天”、“最近 30 天”、“最近三个月”不同时间维度展示病毒查杀事件爆发趋势和病毒 TOP5 排行榜，并展示对应的事件数及终端数； 7. 支持展示全球热点风险事件在网内终端的爆发情况，及时了解、处置网内终端的热点风险事件，并显示影响终端数量； 8.支持全网终端资产清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示。 9.支持对安装了指定版本操作系统、特定应用软件、开放了高危端口的风险主机进行统计，具备对风险主机进行漏洞扫描、安装高危软件的主机列表信息统计导出、高危端口一键封堵的能力。 10.提供对业务系统之间、业务系统内不同应用角色或主机之间、业务系统内相同应用角色之间的访问控制策略配置，并可以图形化显示业务系统、主机及流量详情。 11支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4 地址、MAC地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新； 12. 具备主机发现的能力，管理员可以按照扫描网段、扫描方式、扫描协议、扫描端口对主机进行扫描，来及时发现尚未管控的主机资产，并将所发现的主机列表导出； 13.支持实时监控诱饵文件，能够在勒索病毒修改或加密文件时对该操作进行拦截。 14.支持根据统计周期、终端名称、IP 地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志的查询和检测； 15.支持针对管理控制中心性能，安全事件，勒索病毒事件等邮件告警； 16.一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、恶意代码防范、访问控制、安全审计、访问控制、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果。 17.支持终端管理功能，可以灵活的部署和配置安全策略，支持安全策略模板和安全策略一体化配置，其中安全策略模板可以对指定终端组快速部署安全策略。 18.支持主机分组，并支持主机防病毒系统软件版本的错峰和灰度升级，可以根据云平台实际情况控制云主机同时升级的最大数量，避免大量云主机防病毒软件同时更新造成网络拥堵或 I/O 风暴，并支持主机防病毒软件的启用禁用和重启，在管理平台中心可以直接卸载主机软件。
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表五：综合日志审计

参数性质	序号	具体技术(参数)要求
------	----	------------

	<p>1.性能参数：要求默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥1TB，平均每秒处理日志数≥1200。2U设备，内存至少为8G，至少提供6个千兆电口和日志分析系统软件一套；</p> <p>2.支持自定义首页卡片，支持实时监控日志传输量和日志留存的合规情况。</p> <p>3.支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等</p> <p>4.支持以列表的方式展示告警：告警声音设置：告警过滤策略</p> <p>5.支持全文检索功能，能对系统内的对象提供全文检索功能</p> <p>6.支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。</p> <p>7.支持内置实例管理和报表任务管理</p> <p>8.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。</p> <p>9.支持定义部门和人员的对应关系；支持定义人员与账号的对应关系；</p> <p>10.可通过自定义聚合规则修改日志的聚合归并逻辑规则，提高日志分析效率，支持归并技术，一段时间内对重复日志进行归并；</p> <p>11.支持自定义仪表盘，客户可以选择对应的微件，组成想要关注的仪表展现内容；</p> <p>12.支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；</p> <p>13.支持业务管理配置，可以导出系统内报表、策略、采集器、资产等业务数据，供新设备导入配置，实现快速切换设备</p> <p>14.支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现</p> <p>15.支持集群配置及集群状态监控</p> <p>16.支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用</p> <p>17.支持多种方式的查询检索，包括：日志检索、资产检索、告警检索、事件检索；</p> <p>18.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表六：堡垒机

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1.性能参数：要求提供运维授权数≥50个，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200。硬件参数：内存大小≥4G，硬盘容量≥1T SATA，接口≥6千兆电口。包含安全运维管理软件一套；</p> <p>2. 支持RDP协议的控制台登录控制；</p> <p>3. 支持按加密格式导入、导出运维授权数据，方便授权关系备份以及授权数据迁移；</p> <p>4. 支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问；</p> <p>5. 支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批。</p> <p>6. 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯；</p> <p>7. 内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴；</p> <p>8. 支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。</p> <p>9. 支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯。</p> <p>10.支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人；</p> <p>11. 为适应信息化发展趋势，要求全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计；</p> <p>12. 图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放；</p> <p>13. 支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；</p> <p>14. 支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表七：网络准入

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<p>1.网络层吞吐量≥2Gb，应用层吞吐量≥150Mb，支持用户数≥500，准入终端数≥250，每秒新建连接数≥1000，最大并发连接数≥50000。接口≥4千兆电口。</p> <p>2. 支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能，支持旁路模式，无需更改网络配置，实现上网行为审计及准入控制功能。</p> <p>3. 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；</p> <p>4. 支持DNS透明代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至制定线路；</p> <p>5. 支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等。</p> <p>6. 支持在不安装客户端的状态下，通过流量状况检查10款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复。</p> <p>7. 支持首页分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况。</p> <p>8. 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等。</p> <p>9. 同一个账号，支持与指定数量的多个终端进行自动绑定，支持多人使用同一帐号登录，且支持重复登陆检测机制，限制公共账号的使用人数。</p> <p>10. 支持LDAP、Radius、POP3、Proxy等第三方认证；支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证。</p> <p>11. 支持Web访问质量检测，可针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，可以列表形式展示访问质量差的用户名单并对单用户进行定向web访问质量检测。</p> <p>12. 认证成功用户支持页面跳转：1. 跳转到用户原本输入的URL地址；2.跳转到管理员指定的URL地址；3. 跳转到注销页面；</p> <p>13. 能够与本项目中防毒墙产品实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；</p> <p>14. 支持终端用户可以使用账号绑定的手机号码，接收短信验证码，然后使用手机号码和验证码完成密码认证；支持在终端用户的账号存在微信绑定关系的情况下，PC端的终端用户可以直接使用微信扫码二维码完成密码认证过程，移动端的终端用户，可以直接打开微信扫码完成密码认证过程。</p> <p>15. 为保证应用识别的准确率，设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6500种以上的应用，并保持每两个星期更新一次；</p>
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

附表八：终端安全管理

参数性质	序号	具体技术(参数)要求
------	----	------------

1	<ol style="list-style-type: none"> 1.此次配置终端安全管理软件支持100点终端管理 2.所有功能的导入只需要在终端上安装一个客户端，即可实现所有的功能，确保终端具有良好的兼容性 3.所有功能的管理均通过同一个控制台进行统一管理 4.本系统的服务器端数据库需搭建在MSsql或者MySQL上 5.可通过应用程序、端口、网络地址、通讯方向等参数限制计算机的网络访问权限，可限制单向或双向的通讯方向 6.可自定义网络地址和网络端口类别，方便归类管理 7.可检测内部网络是否有外来计算机非法接入并提供实时报警 8.可与安全检测功能相结合，阻断不合规客户端访问网络，直到终端符合安全检测的要求，才允许访问网络 9.可按“时间”、“到期时间”、“仅离线生效”灵活设置策略 10.当终端的通讯行为触发策略时，支持记录下当时的屏幕画面或锁定计算机 11.可按时间、计算机范围、网络地址（明细、类别）、端口（明细、类别）、流量方向（发送、接收、合计）等方式对网络流量进行统计，并可自定义TOP显示 12.统计结果至少支持列表和图表（柱状图、饼状图）两种显示方式 13.可根据网络地址、端口、流量方向等参数限制计算机的网络流量，达到合理分配带宽的目的 14.可自定义网络地址类别和网络端口类别，方便归类管理 15.支持远程查看客户端计算机当前运行的应用程序、进程、性能、设备管理、系统服务、磁盘管理、共享文件夹、计划任务、用户和组、启动项等，并可对应用程序、进程、系统服务、共享文件夹等进行操作，如可关闭当前运行的应用程序、进程等 16.支持远程卸载客户端计算机安装的软件，并支持对安装项信息进行自定义卸载 17.可点对多远程连接到远端计算机的桌面，直接对计算机进行操作，并支持对远端计算机的键盘、鼠标进行控制 18.支持对客户端下达任务，将客户端全盘文件目录列表或U盘文件列表上传到服务器，支持把客户端某个指定的文件上传到服务器 19.可点对多远程连接到远端计算机的桌面，直接对计算机进行操作，并支持对远端计算机的键盘、鼠标进行控制
说明	打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。

第五章 供应商应当提交的资格、资信证明文件

供应商应提交证明其有资格参加响应和成交后有能力履行合同的相关文件，并作为其响应文件的一部分，所有文件必须真实可靠、不得伪造，否则将按相关规定予以处罚。

1.法人或者其他组织的营业执照等证明文件，自然人的身份证明：

(1) 法人包括企业法人、机关法人、事业单位法人和社会团体法人；其他组织主要包括合伙企业、非企业专业服务机构、个体工商户、农村承包经营户；自然人是指《中华人民共和国民法通则》（以下简称《民法通则》）规定的具有完全民事行为能力、能够承担民事责任和义务的公民。如供应商是企业（包括合伙企业），要提供在工商部门注册的有效“企业法人营业执照”或“营业执照”；如供应商是事业单位，要提供有效的“事业单位法人证书”；供应商是非企业专业服务机构的，如律师事务所，会计师事务所要提供执业许可证等证明文件；如供应商是个体工商户，要提供有效的“个体工商户营业执照”；如供应商是自然人，要提供有效的自然人身份证明。

(2) 这里所指“其他组织”不包括法人的分支机构，由于法人分支机构不能独立承担民事责任，不能以分支机构的身份参加政府采购，只能以法人身份参加。“但由于银行、保险、石油石化、电力、电信等行业具有其特殊性，如果能够提供其法人给予的相应授权证明材料，可以参加政府采购活动”。

2.供应商应符合《中华人民共和国政府采购法》第二十二条规定的条件，提供标准格式的《资格承诺函》。

3.信用记录查询

(1) 查询渠道：通过“信用中国”网站(www.creditchina.gov.cn)和“中国政府采购网”(www.ccgp.gov.cn)进行查询；

(2) 查询截止时点：本项目资格审查时查询；

(3) 谈判小组应当对信用记录查询结果中显示供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商作无效响应处理并将截图存档；

4.采购人或采购代理机构应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示供应商被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商作无效投标处理。

5. 按照谈判文件要求，成交人应当提交的资格、资信证明文件。

第六章 评审

一、评审要求

1. 评标方法

{ { 评标方法谈判 } }

2. 评标原则

2.1 评审活动遵循公平、公正、科学和择优的原则，以谈判文件和响应文件为评审的基本依据，并按照谈判文件规定的评审方法和评审标准进行评审。

2.2 具体评审事项由谈判小组负责，并按谈判文件的规定办法进行评审。

3. 谈判小组

3.1 谈判小组由采购人代表和评审专家共3人以上单数组成，其中评审专家人数不得少于谈判小组成员总数的2/3。

3.2 谈判小组成员有下列情形之一的，应当回避：

(1) 参加采购活动前三年内，与供应商存在劳动关系，或者担任过供应商的董事、监事，或者是供应商的控股股东或实际控制人；

(2) 与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

(3) 与供应商有其他可能影响政府采购活动公平、公正进行的关系；

3.3 谈判小组负责具体评标事务，并独立履行下列职责：

(1) 确认或者制定谈判文件；

(2) 审查供应商的响应文件并作出评价；

(3) 要求供应商对响应文件有关事项作出澄清或者说明，与供应商进行分别谈判；

(4) 编写评审报告；

(5) 确定成交候选人名单，以及根据采购人委托直接确定成交人；

(6) 向采购人、采购代理机构或者有关部门报告评审中发现的违法行为；

(7) 法律法规规定的其他职责。

4. 澄清

谈判小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。

谈判小组、询价小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

4.1 谈判小组不接受供应商主动提出的澄清、说明或更正。

4.2 谈判小组对供应商提交的澄清、说明或更正有疑问的，可以要求供应商进一步澄清、说明或更正。

5. 有下列情形之一的，视为供应商串通响应

5.1 不同供应商的响应文件由同一单位或者个人编制；（不同供应商响应文件上传的项目内部识别码一致）；

5.2 不同供应商委托同一单位或者个人办理响应事宜；

5.3 不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；

5.4 不同供应商的响应文件异常一致或者投标报价呈规律性差异；

5.5不同供应商的响应文件相互混装；

5.6不同供应商的投标保证金为从同一单位或个人的账户转出；

说明：在项目评审时被认定为串通投标的供应商不得参加该合同项下的采购活动

6.有下列情形之一的，属于恶意串通投标

6.1供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其响应文件或者响应文件；

6.2供应商按照采购人或者采购代理机构的授意撤换、修改响应文件或者响应文件；

6.3供应商之间协商报价、技术方案等响应文件或者响应文件的实质性内容；

6.4属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

6.5供应商之间事先约定由某一特定供应商成交、成交；

6.6供应商之间商定部分供应商放弃参加政府采购活动或者放弃成交、成交；

6.7供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商成交、成交或者排斥其他供应商的其他串通行为。

7.投标无效的情形

7.1详见资格性审查、符合性审查和谈判文件其他投标无效条款。

8.废标（终止）的情形

8.1出现下列情形之一的，采购人或者采购代理机构应当终止竞争性谈判采购活动，发布项目终止公告并说明原因，重新开展采购活动：

（1）因情况变化，不再符合规定的竞争性谈判采购方式适用情形的；

（2）出现影响采购公正的违法、违规行为的；

（3）在采购过程中符合谈判要求的供应商或者报价未超过采购预算的供应商不足3家的，但经财政部门批准的情形除外；

（4）法律、法规以及谈判文件规定其他情形。

9.定标

9.1 谈判结束后，谈判小组应当要求所有参加谈判的供应商在规定时间内进行最后报价，采购人从谈判小组提出的成交候选人中根据符合采购需求、质量和价格相等且报价最低的原则确定成交供应商，并将结果通知所有参加谈判的未成交的供应商。

10.其他说明事项

若出现供应商因在投标客户端中对应答点标记错误，导致评审专家无法进行正常查阅的，视为响应文件未实质性响应（未响应）谈判文件该部分要求的，由供应商自行承担责任。

二、政府采购政策落实

1.节能、环保要求

采购的产品属于品目清单范围的，将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购，具体按照本谈判文件相关要求执行

2.对小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除

依照《政府采购促进中小企业发展管理办法》、《关于政府采购支持监狱企业发展有关问题的通知》和《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》的规定，凡符合要求的小型、微型企业、监狱企业或残疾人福利性单位，按照以下比例给予相应的价格扣除：（监狱企业、残疾人福利性单位视同为小、微企业）

合同包1（网络等级保护二级设备）

序号	情形	适用对象	价格扣除比例	计算公式
1	小型、微型企业，监狱企业，残疾人福利性单位	非联合体	10%	本项目对属于小型和微型企业的投标人的投标报价给予相应百分比的扣除，用扣除后的价格参与评审。残疾人福利性单位视同小型、微型企业，享受同等价格扣除，但同时属于残疾人福利性单位和小微企业的，不重复价格扣除。
注：（1）上述评标价仅用于计算价格评分，成交金额以实际投标价为准。（2）组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。				

3.价格扣除相关要求

3.1所称小型和微型企业应当同时符合以下条件：

- （1）符合中小企业划分标准；
- （2）提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。
- （3）中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准。
- （4）小型、微型企业提供中型企业制造的货物的，视同为中型企业。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

3.2在政府采购活动中，供应商提供的货物、工程或者服务符合下列情形的，享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策：

- （1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；
- （2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；
- （3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动民法典》订立劳动合同的从业人员。

在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受《政府采购促进中小企业发展管理办法》规定的中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

3.3供应商属于小微企业的应填写《中小企业声明函》；监狱企业须供应商提供由监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；残疾人福利性单位应填写《残疾人福利性单位声明函》，否则不认定价格扣除。

说明：供应商应当认真填写声明函，若有虚假将追究其责任。

3.4提供供应商的《中小企业声明函》、《残疾人福利性单位声明函》（格式后附，不可修改），未提供、未盖章或填写内容与相关材料不符的不予价格扣除。

三、评审程序

1.资格性审查和符合性审查

1.1资格性审查。依据法律法规和谈判文件的规定，对响应文件中的资格证明文件等进行审查，以确定响应供应商是否具备响应资格。（详见后附表一资格性审查表）

1.2符合性审查。依据谈判文件的规定，从响应文件的有效性、完整性和对谈判文件的响应程度进行审查，以确定是否对谈判文件的实质性要求作出响应。（详见后附表二符合性审查表）

1.3资格性审查和符合性审查中凡有其中任意一项未通过的，评审结果为未通过，未通过资格性审查、符合性审查的投标单位按无效投标处理。

2.谈判

(1) 谈判小组应当通过随机方式确定参加谈判供应商的谈判顺序，谈判小组所有成员应当集中与单一供应商分别进行谈判，并给予所有参加谈判的供应商平等的谈判机会。

(2) 谈判内容主要包括：针对本项目的技术、服务要求以及合同草案条款等；谈判文件不能详细列明采购标的的技术、服务要求的，需经谈判由供应商提供最终设计方案或解决方案；其它需要谈判的事项。

在谈判过程中，谈判小组可以根据谈判文件和谈判情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动谈判文件中的其他内容。实质性变动的内容，须经采购人代表确认。

对谈判文件作出的实质性变动是谈判文件的有效组成部分，谈判小组应当及时、同时通知所有参加谈判的供应商。

供应商应当按照谈判文件的变动情况和谈判小组的要求进行最终报价或重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

3.最后报价

3.1谈判结束后，谈判小组应当要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价是供应商响应文件的有效组成部分。如实质性响应供应商未按规定要求和时间递交最后报价，将以该供应商提交的初始报价作为其最后报价。

3.2已提交响应文件的供应商，在提交最后报价之前，可以根据谈判情况退出谈判。

3.3最后报价逾时不交的（超过最后报价时限要求的）、最后报价未携带有效CA锁的将视为供应商自动放弃最后报价。

3.4注：最后报价应当按照本项目采购文件的相关要求，在最后报价现场对总报价和分项报价进行明确，请各供应商在参加谈判前对可能变动的报价进行准备、计算。

4.政府采购政策功能落实

对于小型、微型企业、监狱企业或残疾人福利性单位给予价格扣除。

5.汇总、排序

5.1响应文件满足谈判文件全部实质性要求，且进行政府采购政策落实的价格扣除后，对最后响应报价进行由低到高排序，确定价格最低的供应商为成交人候选人。价格相同的，按技术指标顺序排列确定，以上均相同的由采购人确定。

表一资格性审查表

合同包1（网络等级保护二级设备）

具有独立承担民事责任的能力	在中华人民共和国境内注册的法人或其他组织或自然人，投标时提交有效的营业执照（或事业法人登记证或身份证等相关证明）副本复印件。
有依法缴纳税收和社会保障资金的良好记录	按资格承诺函提供
具有良好的商业信誉和健全的财务会计制度	按资格承诺函提供
履行合同所必须的设备和专业技术能力	按资格承诺函提供
参加采购活动前3年内，在经营活动中没有重大违法记录	按资格承诺函提供

信用记录	对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单、信用报告进行查询；应当按照查询渠道、查询时间节点、查询记录内容进行查询，并存档。对信用记录查询结果中显示投标人被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商作无效响应处理。
供应商必须符合法律、行政法规规定的其他条件	按资格承诺函提供
落实政府采购政策需满足的资格要求	无

表二符合性审查表：

合同包1（网络等级保护二级设备）

报价	报价（包括分项报价和总报价）只能有一个有效报价且不超过采购预算，不得缺项、漏项。
响应文件规范性、符合性	响应文件的签署、盖章、删除、插字、公章等符合采购文件的要求；响应文件的格式、文字等符合采购文件要求或无实质性影响。
主要商务条款	按要求提供标准格式的“主要商务要求承诺书”
联合体投标	非联合体投标不提供。
技术部分实质性内容	项目经办人按照具体情况进行调整。3.货物类：明确所投标的产品品牌、规格型号；响应文件对谈判文件提出的要求和条件作出明确响应并满足谈判文件全部实质性要求。4.工程类：（1）工期，符合招标文件要求；（2）工程质量，达到合格以上标准；（3）已标价工程量清单，包含所有工程内容；3.服务类：依据采购文件的规定，从响应文件的有效性、完整性和对采购文件的响应程度，主要是对服务需求的响应程度进行检查，以确定是否对采购文件的实质性要求作出响应，否则响应无效。4.节能产品认证证书。货物或工程量清单施工材料中，所投设备属于《节能产品政府采购品目清单》中强制采购产品范围的（如台式计算机，便携式计算机，平板式微型计算机，激光打印机，针式打印机，液晶显示器，制冷压缩机，空调机组，专用制冷、空调设备，镇流器，空调机，电热水器，普通照明用双端荧光灯，电视设备，视频设备，便器，水嘴等为政府强制采购的产品），供应商应提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则其响应文件无效；信息安全产品，供应商响应产品应为经国家认证的信息安全产品，并提供由中国信息安全认证中心按国家标准认证颁发的有效认证证书，否则其响应文件无效。
投标承诺书	按要求提供标准格式的“投标承诺书”
其他要求	

表三详细评审表：

第七章 响应文件格式与要求

供应商提供响应文件应按照以下格式及要求进行编制，且不少于以下内容。

响应文件封面

(项目名称)

响应文件封面

(正本/副本)

项目编号：**[230230]KDC[TP]20210009**

所投采购包：第 包

(供应商名称)

年 月 日

响应文件目录

- 一、投标承诺书
- 二、资格承诺函
- 三、授权委托书
- 四、主要商务要求承诺书
- 五、技术偏离表
- 六、中小企业声明函
- 七、监狱企业
- 八、残疾人福利性单位声明函
- 九、分项报价明细表
- 十、保证金
- 十一、联合体协议书
- 十二、项目实施方案、质量保证及售后服务承诺等
- 十三、项目组成人员一览表
- 十四、供应商业绩情况表
- 十五、各类证明材料

格式一：

投标承诺书

采购单位、克东县公共资源交易综合服务中心：

1.按照已收到的 项目（项目编号： ）谈判文件要求，经我方（供应商名称）认真研究投标须知、合同条款、技术规范、资质要求和其它有关要求后，我方愿按上述合同条款、技术规范、资质要求进行投标。我方完全接受本次谈判文件规定的所有要求，并承诺在中标后执行谈判文件、响应文件和合同的全部要求，并履行我方的全部义务。我方的最终报价为总承包价，保证不以任何理由增加报价。

2.我方同意谈判文件关于投标有效期的所有规定。

3.我方郑重声明：所提供的响应文件内容全部真实有效。如经查实提供的内容、进行承诺的事项存在虚假，我方自愿接受有关处罚，及由此带来的法律后果。

4.我方将严格遵守《中华人民共和国政府采购法》、《中华人民共和国民法典》等有关法律、法规规定，如有违反，无条件接受相关部门的处罚。

5.我方同意提供贵方另外要求的与其投标有关的任何数据或资料。

6.我方将按照谈判文件、响应文件及相关要求、规定进行合同签订，并严格执行和承担协议和合同规定的责任和义务。

7.我单位如果存在下列情形的，愿意承担取消中标资格、接受有关监督部门处罚等后果：

- （1）中标后，无正当理由放弃中标资格；
- （2）中标后，无正当理由不与招标人签订合同；
- （3）在签订合同时，向招标人提出附加条件或不按照相关要求签订合同；
- （4）不按照谈判文件要求提交履约保证金；
- （5）要求修改、补充和撤销响应文件的实质性内容；
- （6）要求更改谈判文件和中标结果公告的实质性内容；
- （7）法律法规和谈判文件规定的其他情形。

详细地址：

邮政编码：

电话：

电子函件：

供应商开户银行：

账号/行号：

供应商法人签字：（加盖公章）

年 月 日

格式二：

资格承诺函

我单位作为本次采购项目的供应商，根据采购文件要求，现郑重承诺如下：

（一）符合《中华人民共和国政府采购法》第二十二条规定的条件；

- 1.具有独立承担民事责任的能力；
- 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；
- 5.参加本次政府采购活动前三年内，在经营活动中没有重大违法记录；
- 6.符合国家法律、行政法规规定的其他条件。

（二）我公司作为本项目参加政府采购活动的供应商、法定代表人/单位负责人近3年内不具有行贿犯罪记录。

（三）我公司在截至响应截止日未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

本公司对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我公司愿意接受以提供虚假材料谋取成交追究法律责任。

供应商（单位盖章）：

日 期：

格式三：

授权委托书

本人_____（姓名）系_____（供应商名称）的法定代表人，现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改招标项目响应文件、签订合同和处理有关事宜，其法律后果由我方承担。委托期限：_____。

代理人无转委托权。

投标人：_____（加盖公章）

法定代表人：_____（签字）

授权委托人：_____（签字）

法定代表人身份证扫描件 国徽面	法定代表人身份证扫描件 人像面
授权委托人身份证扫描件 国徽面	授权委托人身份证扫描件 人像面

_____年_____月_____日

格式四：

主要商务要求承诺书

我公司承诺可以完全满足本次采购项目的**所有**主要商务条款要求（如标的提供的时间、标的提供的地点、投标有效期、采购资金支付、验收要求、履约保证金等）。若有不符合或未按承诺履行的，后果和责任自负。

如有优于谈判文件主要商务要求的请在此承诺书中说明。

具体优于内容（如标的提供的时间、地点，质保期等）。

特此承诺。

供应商名称：（加盖公章）

_____年 月 日

格式五：

技术偏离表

序号	标的名称	招标技术要求	投标人提供响应内容	偏离程度	备注
1		★ 1.1			
		1.2			
				
2		★ 2.1			
		2.2			
				
.....					

说明：

1. 供应商应当如实填写上表“供应商提供响应内容”处内容，对谈判文件提出的要求和条件作出明确响应，并列明具体响应数值或内容，只注明符合、满足等无具体内容表述的，将视为未实质性满足谈判文件要求。

2. “偏离程度”处可填写满足、响应或正偏离、负偏离。

3. 佐证文件名称及所在页码：系指能为投标产品提供技术参数佐证或进一步提供证据的文件、资料名称及相关佐证参数所在页码。如直接复制采购文件要求的参数但与佐证材料不符的，为无效投标。

4.上表中“招标技术要求”应详细填写招标要求。

格式六：（不属于可不填写内容或不提供）

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：

中小企业声明函（货物）

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，提供的货物全部由符合政策要求的中小企业制造。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）行业；制造商为（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）行业；制造商为（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：

格式七：（不属于可不填写内容或不提供）

监狱企业

提供由监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

格式八：（不属于可不填写内容或不提供）

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（加盖公章）：

日期：

格式九：

分项报价明细表

序号	标的名称	品牌、规格型号/主要服务内容	制造商名称	产地	数量	单位	单价 (元)	总价 (元)
1								
2								
3								
...								

注：采用电子招投标的项目无需编制该表格，投标供应商应在投标客户端【报价部分】进行填写，投标客户端软件将自动根据供应商填写信息在线生成开标一览表（首轮报价表、报价一览表）或分项报价表，若在响应文件中出现非系统生成的开标一览表（首轮报价表、报价一览表）或分项报价表，且与投标客户端生成的开标一览表（首轮报价表、报价一览表）或分项报价表信息内容不一致，以投标客户端生成的内容为准。

格式十：

投标保证金

供应商应在此提供保证金的凭证的复印件。

格式十一：（不属于可不填写内容或不提供）

联合体协议书

_____（所有成员单位名称）自愿组成_____（联合体名称）联合体，共同参加_____（项目名称）招标项目投标。现就联合体投标事宜订立如下协议。

- 1.（某成员单位名称）为（联合体名称）牵头人。
2. 联合体各成员授权牵头人代表联合体参加投标活动，签署文件，提交和接收相关的资料、信息及指示，进行合同谈判活动，负责合同实施阶段的组织和协调工作，以及处理与本招标项目有关的一切事宜。
3. 联合体牵头人在本项目中签署的一切文件和处理的一切事宜，联合体各成员均予以承认。联合体各成员将严格按照谈判文件、响应文件和合同的要求全面履行义务，并向招标人承担连带责任。
4. 联合体各成员单位内部的职责分工如下：_____。
5. 本协议书自所有成员单位法定代表人或其授权代表签字或盖单位章之日起生效，合同履行完毕后自动失效。
6. 本协议书一式_____份，联合体成员和招标人各执一份。

协议书由法定代表人签字的，应附法定代表人身份证明；由授权代表签字的，应附授权委托书。

联合体牵头人名称：_____（加盖公章）
法定代表人或其授权代表：_____（签字）
联合体成员名称：_____（加盖公章）
法定代表人或其授权代表：_____（签字）

_____年_____月_____日

格式十二：

项目实施方案、质量保证及售后服务承诺等内容和格式自拟。

格式十三：

项目组成人员一览表

序号	姓名	本项目拟任职务	学历	职称或执业资格	身份证号	联系电话
1						
2						
3						
.....						

按谈判文件要求在本表后附相关人员证书。

注：

- 1.本项目拟任职务处应包括：项目负责人、项目联系人、项目服务人员或技术人员等。
- 2.如供应商中标，须按本表承诺人员操作，不得随意更换。

格式十四：

供应商业绩情况表

序号	使用单位	业绩名称	合同总价	签订时间
1				
2				
3				
4				
...				

供应商根据上述业绩情况后附销售或服务合同复印件。

格式十五：

各类证明材料

- 1.谈判文件要求提供的其他资料。
- 2.供应商认为需提供的其他资料。