江苏省政府采购合同

项目名称：传染病监测预警与应急指挥能力提升项目

项目编号：JSZC-320200-JZCG-G2024-0113

甲方：（买方、需方、采购人）无锡市疾病预防控制中心

乙方：（卖方、供方、供应商）江苏移动信息系统集成有限公司

甲、乙双方根据无锡市公共资源交易中心传染病监测预警与应急指挥能力提升项目公开招标的结果，签署本合同。

一、合同内容

1.1 标的名称：传染病监测预警与应急指挥能力提升项目

1.2 标的质量：按招标文件确定的事项和中标人投标文件执行

1.3 标的数量（规模）：按招标文件确定的事项和中标人投标文件执行

1.4 履行时间（期限）：IPSEC/SSLVPN（网关设备）、服务器密码机设备、签名验签服务器、防火墙、视频会议系统自验收合格之日起五年，软件自验收合格之日起三年

1.5 履行地点：无锡市梁溪区金城路 499 号

1.6 履行方式：按招标文件确定的事项和中标人投标文件执行

1.7 包装方式：按招标文件确定的事项和中标人投标文件执行

二、合同金额

2.1 本合同金额为（大写）：伍拾叁万元整（530000 元）人民币（含税价）。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供使用货物(包含与货物相关的服务)的有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同货物（包含与货物相关的服务）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知

识产权的起诉。一旦出现侵权，由乙方负全部责任。

（注：采购项目如涉及采购标的的知识产权归属、处理的，如订购、设计、定制开发的信息化建设项目等，应当约定知识产权的归属和处理方式）

五、产权担保

5.1 乙方保证所交付的货物（包含与货物相关的服务）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 乙方交纳人民币/元作为本合同的履约保证金。（不得超过合同金额的10%）

6.2 合同履行结束后，甲方应及时退还交纳的履约保证金。

6.2.1 履约保证金退还方式：/

6.2.2 履约保证金退还时间：/

6.2.3 履约保证金退还条件：/

6.2.4 履约保证金不予退还的情形：/

七、合同转包或分包

7.1 乙方不得将合同标的转包给他人履行。

7.2 乙方应按招标文件要求，如项目不允许分包的，乙方不得将合同标的分包给他人履行；如项目允许分包的，乙方应当按照投标文件中提供的分包意向协议履行合同。

7.3 乙方如有转包或未经甲方同意的分包行为，甲方有权给予终止合同。

八、合同款项支付

8.1 合同款项的支付方式及进度安排

8.1.1 预付款支付时间：合同签订生效后10个工作日内，到货安装调试完成并验收合格，支付合同总金额的30%。

8.1.2 尾款支付时间：验收合格稳定运行90天后付清其余合同总金额70%的尾款。

8.2 当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

九、税费

9.1 本合同执行中相关的一切税费均由乙方负担。

十、质量保修范围和保修期及售后服务

10.1 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

10.2 乙方提供的货物在质量期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

10.3 如在使用过程中发生质量问题，乙方在接到甲方通知后在 4 小时内到达甲方现场。

10.4 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

10.5 上述的货物免费保修期为 IPSEC/SSLVPN（网关设备）、服务器密码机设备、签名验签服务器、防火墙、视频会议系统自验收合格之日起五年，软件自验收合格之日起三年，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

十一、项目验收

11.1 甲方依法组织履约验收工作。

11.2 甲方在组织履约验收前，将根据项目特点制定验收方案，明确履约验收的时间、方式、程序等内容，并可根据项目特点对服务期内的服务实施情况进行分期考核，综合考核情况和服务效果进行验收。乙方应根据验收方案内容做好相应配合工作。

11.3 对于实际使用人和甲方分离的项目，甲方邀请实际使用人参与验收。

11.4 如有必要，甲方邀请参加本项目的其他供应商或第三方专业机构及专家参与验收，相关意见将作为验收书的参考资料。

11.5 甲方成立验收小组，按照采购合同的约定对乙方的履约情况进行验收。验收时间、验收标准见招标文件验收内容。验收时，甲方按照采购合同的约定对

每一项技术、商务要求的履约情况进行确认。验收结束后,验收小组出具验收书,列明各项标准的验收情况及项目总体评价,由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料存档备查。

11.6 验收合格的项目,甲方根据采购合同的约定及时向乙方支付合同款项。验收不合格的项目，甲方依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《民法典》。乙方在履约过程中有政府采购法律法规规定的违法违规情形的,甲方将及时报告本级财政部门。

十二、货物的包装、发运及运输

12.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。乙方对货物的包装应符合《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》的规定。

12.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

12.3 乙方在货物发运手续办理完毕后 24 小时内或货到甲方 48 小时前通知甲方，以准备接货。

12.4 货物在交付甲方前发生的风险均由乙方负责。

12.5 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

十三、违约责任

13.1 甲方无正当理由拒收货物的,甲方向乙方偿付拒收货款总值__/__的违约金。

13.2 甲方无故逾期验收和办理货款支付手续的,甲方应按逾期付款总额每日__/__向乙方支付违约金。

13.3 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期 10 个工作日不能交货的,甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的,乙方应向甲方支付合同总值__/__的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

13.4 乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定

及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

十四、不可抗力事件处理

14.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

14.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

14.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十五、解决争议的方法

15.1 甲乙双方因合同签订、履行而发生的一切争议，应通过友好协商解决。如协商不成由甲方住所地人民法院管辖。

十六、合同生效及其它

16.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

16.2 本合同未尽事宜，遵照《民法典》、《政府采购法》有关条文执行。

16.3 本合同正本一式两份，具有同等法律效力，甲方、乙方各执一份。

甲方：

地址：

法定代表人或授权代表：

联系电话：

乙方：

地址：南京市虎踞路 59 号

法定代表人或授权代表：

联系电话：13800250222

乙方户名：江苏移动信息系统集成有限公司

开户银行：中国银行股份有限公司南京云锦路支行

账号：479361758530

签订日期：2024 年 8 月 2 日

附件 1、保密责任书

保密责任书

为保证国家秘密安全和甲方技术、业务数据秘密安全，根据《中华人民共和国保守国家秘密法》和国家有关保密工作的规定，订立本保密责任书。乙方在本项目实施过程中必须严格执行以下要求：

（一）严格遵守国家保密法律、法规，严格执行保密要求。

（二）负责对参与本项目人员的审查，确保人员符合国家保密法的有关规定。

（三）对员工进行保密教育和培训，及时传达有关保密工作的规定及管理规章制度。

（四）对施工中接触到的秘密事项承担保密责任，承担失泄密的一切法律责任。

（五）乙方人员不得进入自身施工和生活区域以外区域。

（六）不得在本项目现场进行拍照、录音、录像。

（七）乙方对甲方提供的图纸、技术资料和接触到的甲方技术、业务数据秘密保密，采取相应的保密措施。未经甲方允许，乙方不得将本项目图纸、技术资料和接触到的甲方技术、业务数据秘密复制或提供给第三方使用，亦不得用于其它项目。

（八）乙方不遵守以上规定，甲方发现后可以对乙方进行经济处罚，造成甲方损失的，乙方赔偿全部损失，造成失泄密的，追究乙方一切法律责任。

甲方：（盖单位章）　　乙方：（盖单位章）

法定代表人或其委托代理人：　　法定代表人或其委托代理人：

（签字）　　（签字）

时间：2024年8月2日

附件 2、项目清单

序号	名称	品牌型号	性能指标	数量	产地	质保期
1	IPSEC/SSLVPN（网关设备）	天融信TopVPN 6000（FT-B20）	硬件配置： 国产化 CPU 和国产化操作系统； 内存:16G，存储空间:机械硬盘 4TB；配置 6 个千兆电口，4 个千兆光插槽，2 个扩展槽位；冗余电源；IPSEC 国密算法吞吐率 800Mbps，IPSEC VPN 隧道数 6000 ，SSL 吞吐率 300Mbps，SSL 最大并发用户数 3000；200 个 SSL VPN 的客户端许可。 基本要求： VPN 网关设备须与省级设备兼容互认。 VPN 网关设备应支持已发放使用的用户数字证书和升级后的数字证书。 VPN 网关设备应支持不同品牌互联互通，兼容互认，满足商用密码相关标准。 网络适应性： 支持透明、路由、混合模式；支持基于源/目的地址、端口、协议及接口的策略路由； 支持 Vlan、Vlan Trunk，支持 802.1Q、ISL 的封装和解封； 支持 vlan-vpn 功能，能对报文进行二次基于 802.1Q 封装； 支持自有 DDNS 动态域名注册，支持使用域名进行动态寻址，支持使用域名进行隧道定义及协商，支持使用域名进行集中认证和管理 ； 支持虚拟 DNS 功能，网关可提供 DNS 服务，支持自定义内网服务器域名； 用户管理： 支持 IPSEC 与 SSL 使用同一套用户认证、管理系统；管理用户数超过 15000； 支持用户与手机号码、PC 硬件特征码、手机硬件特征码、IP、MAC 等硬件信息的绑定，支持自动审批和人工审批两种模式； 支持自定义同一 VPN 账号可登录的终端设备数量； 支持主从认证账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定； SSL VPN 认证与授权： 符合国密局制定的《SSL VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4； 客户端支持主流 Windows 系统、MAC 系统、Linux 系统（含 Cent OS、Ubuntu、银河麒麟、优麒麟等）；兼容多种类型浏览器，包括 IE6、7、8、9、10、11，Chrome、Opera 、Safari、	1	中国	5 年

			Firefox； 支持双机热备模式下的授权漂移，仅需采购一套接入许可； 支持 SSL VPN 会话状态监测； 支持 WebCache 功能；对 web 页面进行数据优化，减少不必要的数据传输； 支持基于 Android/ IOS 平台的第三方软件开发包（SDK），用于封装第三方应用软件（APP），无需安装独立客户端，即可实现数据加密传输，业务安全接入； 支持虚拟门户（PORTAL）风格自定义，可替换图片、文本等对资源进行自定义说明。 支持口令复杂度设置、支持首次登录修改口令、支持密码找回功能；支持多点登录地点数设置、支持登录时间、登录地址范围控制； 可信接入： 支持接入主机的安全检查，包括安装的软件、进程、端口、服务、注册表、操作系统及补丁、文件、网卡等，支持接入前检查、接入后检查、定时检查等策略；支持可信接入分级授权； IPSEC VPN： 支持 ESP/AH/IKE/NATT 等标准 IPSEC 协议，支持隧道模式、传输模式，且网关所有功能都必须是基于标准 IPSEC 协议； 符合国密局制定的《IPSEC VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4； 支持国密算法、国际算法、国密/国际混合算法的自由切换； 网络安全性： 支持网络隔离功能，用户登录 SSL VPN 后，只能访问授权资源，不能进行其他的网络访问，确保隧道数据安全； 可基于区域、VLAN、IP 地址、MAC 地址、端口和协议、时间、用户角色等的访问控制，并支持访问控制策略分组管理； 系统管理： 支持 Welf、Syslog 等多种日志格式的输出，可对日志进行加密传输； 支持双操作系统故障切换，保障单台设备的高可用性；支持双系统升级，支持 TFTP、Webui、Ftp 升级； 提供轮流、权重轮流、最少连接、加权最少连接、源/目的地址 HASH 等 11 种负载均衡方式。 产品资质要求： 具备国家密码管理局颁发的《商用密码产品认证证书》； 质保服务： 原厂 5 年质保服务，原厂工程师 5 年上门服务			

2	服务器密码机设备	天融信 TopCSP（FT-B40）	硬件配置： 国产化 CPU 和国产化操作系统，内存 32G,机械硬盘 4T，6 个千兆电口，4 个 SFP 插槽,2 个扩展槽位；冗余电源。 性能要求　　SM2 算法最大密钥生成速率 10000 对/秒 ，SM2 算法最大签名速率 8500 次/秒 ，SM2 算法最大验签速率 6000 次/秒 ，SM3 算法完整性校验最大吞吐率 500Mbps，SM4 算法加解密最大吞吐率 600Mbps，RSA 算法最大密钥生成速率 120 对/秒，1024 位 RSA 算法最大签名速率 3000 次/秒 ，1024 位 RSA 算法最大验签速率 55000 次/秒 ，SHA1 算法加解密最大吞吐率 1500Mbps ，SHA2 算法加解密最大吞吐率 1200Mbps ，DES 算法加解密最大吞吐率 1100Mbps，3DES 算法加解密最大吞吐率 500Mbps，AES 算法加解密最大吞吐率 2500Mbps； 基本要求： 符合 GM/T 0030-2014《服务器密码机技术规范》，满足 GM/T 0028-2014《密码模块安全技术要求》第二级要求。 基本功能： 通过数字签名可以保证信息传输的完整性、对发送者进行源认证以及防抵赖支持用户自行修改单点登陆的账户信息； 支持三层密钥结构：管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥； 具备四路随机噪声源，采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数； 符合 GM/T 0018-2012《密码设备应用接口规范》标准，支持 WINDOWS、LINUX 系统平台，提供 JAVA、C 语言的接口，具备高兼容性； 业务配置： 支持白名单 IP 授权登录管理页面；业务通信支持国际和国密协议； 应用接口： 支持多操作系统 Linux、Windows； 支持 API 接口描述，包括接口类别、接口实例，根据所选择的具体接口，显示该接口函数的名称、参数、以及示例 demo； 日志管理： 支持配置管理日志、系统日志、业务日志审计，支持按日志类型、时间、级别、关键词等分类查询；支持日志级别自定义配置； 系统管理： 支持三元管理；支持手动与本地同步两种方式修改系统时	1	中国	5 年

			间； 支持基于 TFTP 服务器、FTP 服务器和本地方式升级设备的系统软件；支持负载均衡模式多机并行； 可支持单机上扩展多块密码卡； 可展示与其建立连接的所有连接的基本信息，包括协议、本地 IP/端口、连接 IP/端口以及连接状态； 支持对配置文件的备份、下载、删除、恢复和上载； 支持对部分配置本地和异地的批量导出和导入； 产品资质要求： 具备国家密码管理局颁发的《商用密码产品认证证书》； 质保服务： 原厂 5 年质保服务，原厂工程师 5 年上门服务			
3	签名验签服务器	天融信 TopSVS（FT-B20）	硬件配置： 国产化 CPU 和国产化操作系统，内存 32G,机械硬盘 4T，6 个千兆电口，4 个 SFP 插槽,2 个扩展槽位,双电源。 性能要求： SM2 密钥生成 5400 对/秒,SM2 算法签名 8100 次/秒,SM2 算法验签 2900 次/秒，SM2 制作信封 1500 次/秒，SM2 解密信封 2000 次/秒，SM3 算法 470Mbps，SM4 算法 1350Mbps，RSA 密钥生成 150 对/秒,1024 位 RSA 签名 7300 次/秒,1024 位 RSA 验签 8200 次/秒，1024 位 RSA 制作信封 9300 次/秒，1024 位 RSA 解密信封 6800 次/秒，SHA1 加解密 1500Mbps，SHA2 加解密 1400Mbps，DES 加解密 1300Mbps，3DES 加解密 700Mbps，AES 加解密 2700Mbps； 基本要求： 应符合 GM/T 0029-2014《签名验签服务器技术规范》，满足 GM/T 0028-2014《密码模块安全技术要求》第二级要求。 身份认证功能： 实现基于数字证书的身份认证，支持不同 CA 的证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。 文件签名与验证： 对文件提供数字签名和数字签名验证功能。 证书有效性验证功能： 提供 CRL/OCSP 等多种方式的证书有效性验证。	1	中国	5 年

			获取证书信息功能： 提供证书解析功能，获取证书中的任意主题信息以及扩展项信息。 证书存储功能： 可实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书。 证书动态黑名单功能： 可以自动更新黑名单，采用动态更新方式，无需重启服务。 服务端热备负载： 支持服务端负载均衡功能，来解决不能对外提供大数据量服务的问题，即多台机器负载时，多台机器能够同时对外提供一样的服务来处理大数据量，能够提供一个高性能的服务。 产品资质要求： 具备国家密码管理局颁发的《商用密码产品认证证书》； 质保服务： 原厂 5 年质保服务，原厂工程师 5 年上门服务			

4	防火墙	天融信NGFW4000-UF(千兆)V3	硬件要求： 国产化 CPU 和国产化操作系统；配置 1 个管理口、2 个扩展槽位、6 个千兆电口和 4 个千兆光口,冗余电源；16 内存、4TB 硬盘。 软件　　所投产品必须为下一代防火墙,非 UTM 或其他产品,产品采用多核及自主知识产权的多核并行安全操作系统构成；支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择），不得在 WEB 维护界面中设置系统切换选项；系统具有良好的可扩展性，能够扩展支持病毒防御、入侵防御、应用识别、WEB 分类库过滤、APT 防御、IPSEC VPN 与 SSL VPN 功能； 性能　　防火墙网络层吞吐量(双向)：IPv47121.831Mbps，IPv67198.180Mbps；应用层吞吐量(单向)：IPv42076.333Mbps，IPv62079.667Mbps，TCP 新建连接速率：IPv410.666 万/秒，IPv69.998 万/秒，TCP 并发连接数：IPv4300.000 万，IPv6300.000 万 网络接入： 支持路由、交换、虚拟线、Listening、混合工作模式； 支持根据入接口、源/目的 IP 地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由； 支持链路聚合，可根据源/目的 mac、源/目的 IP、源/目的端口、五元组、端口轮询等条件提供不少于 10 种链路负载算法； 安全控制： 支持一体化安全策略配置，通过一条策略实现五元组、源 MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、WAF、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置，简化用户管理。 内置 P2P 应用、加密应用、数据库应用、工控物联网协议等应用特征库； 支持应用特征库在线或本地更新，支持自定义应用特征； 内置内容过滤功能，可对 FTP 上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤； 支持将五元组、源 MAC、地址范围、应用、用户等加入静态黑名单，可与 URL 过滤、病毒过滤、防代理功能进行联动实	1	中国	5 年

			现动态黑名单封锁，支持静态和动态黑名单命中统计和监控； 内置防代理功能，阻断网络用户通过代理主机进行攻击、共享上网等行为； 安全防护： 支持独立的入侵防护规则特征库，规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，特征总数在5000条以上；能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； 支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御；支持至少2种专业反病毒厂商的病毒特征库，病毒特征库规模超过400万 支持DNS FLOOD防护，能对DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒、DNS格式等攻击提供DNS REPLY源认证、源限速、目的限速、域名限速等综合防护手段； 接入安全： 支持IPSec VPN功能，支持AES、DES、3DES、MD5、SHA-1等VPN加密、认证算法，支持对隧道内网络流量进行监控展示； 支持SSL VPN功能，满足远程用户安全接入内网，支持windows、Android、iOS等远程客户端接入； 系统管理： 支持多个配置文件并存，配置文件备份能力不少于4个；配置文件支持选择部分配置和全部配置导入导出；支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于5个； 数据中心： 支持独立审计策略，可对URL地址、网页标题、网页内容、邮件行为、邮件内容、FTP上传/下载行为及文件内容进行审计； 提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET等上网行为以及用户上网流量时长等内容进行查询； 支持日志本地存储，可对不同类型日志设置存储空间，支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数； 质保服务： 原厂5年质保服务，原厂工程师5年上门服务			

5	防病毒系统	天融信 TopEDR	基本要求： 终端威胁防御系统基础组件，包含实现系统的集中管理、病毒查杀，增强勒索病毒防护、勒索病毒诱捕、策略配置、报表查看等功能，防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能；客户端系统支持 Windows XP/VISTA/WIN7/WIN8/WIN10、WindowsServer 和 LinuxServer， 配置 400 个 PC 端授权许可；3 年特征库升级服务； 管理架构： 系统支持全中文界面，B/S 架构。管理员只需通过浏览器登录控制中心，即可对系统进行管理； 操作系统支持： 至少支持 WindowsXP、Windows 7、Windows 8、Windows 10 等 32 位/64 位终端操作系统，支持 Windows2003、Windows2008、Windows2012 等 32 位/64 位服务器操作系统。同时需支持 Linux 操作系统以及中标麒麟、银河麒麟等国产操作系统； 服务端快速恢复： 服务端采用 Docker 部署方式，能够快速恢复，横向扩展，可移植性强； 客户端安装： 客户端安装支持本地安装，WEB 安装，域推送安装方式； 平台管控 能够对客户端进行统一管理，统一下达指令； 可视化展示： 支持控制中心直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示； 终端管理： 控制中心支持实时显示客户端的状态及终端基本信息，包括客户端在线状态、安全服务状态、终端 IP 地址、MAC 地址、上线时间、操作系统名称、版本信息、系统类型、病毒库时间等信息； 支持客户端主动升级及平台即时/定时推送升级；支持全网/以分组、标签为单位/指定某些客户端定制不同版本升级包，实现差异管理、灰度升级； 权限控制： 支持多管理员管理，同权限管理员共享数据。 支持控制中心访问控制，包含 WEB 访问控制定制超时时间、登录重试次数、IP 锁定时长及解锁，IP 访问控制指定具体	1	中国	3 年

			IP 可访问控制中心 病毒查杀： 至少支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力。并具备空闲查杀、断点查杀、后台查杀等功能； 要求对流行病毒的检测能力必须超过 98%的检出率，超过 98%的清除率，小于 0.1%的误报率； 针对恶意行为的的监控，能够提供增强勒索病毒防护，同时可以开启勒索病毒诱捕。 终端防御： 支持虚拟补丁功能，针对网络数据流的深层分析，检测入站流量并保护应用程序免受攻击，有效阻止勒索病毒等高危威胁的入侵。 支持内容拦截主动防御，当文件被执行、修改、访问时，反病毒引擎对相应文件进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作。 支持终端防火墙功能，支持包括但不限于通过协议（TCP、UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW），端口号，IP 地址、进出口方向等控制规则对终端进行防护，从网络层保护终端安全。 客户端管理： 能够设置终端卸载或脱离管理中心时要输入的密码，防止终端用户随意脱离保护； 客户端提供控制中心管理所需的相关数据信息，通讯加密； 支持客户端安全日志详细追踪及导出； 服务： 提供原厂 3 年软件升级服务，提供原厂工程师 3 年上门服务，提供 400 个终端替换原有防护软件安装部署服务。			

6	内网终端安全管理系统	天融信TSM-TopDesk3.0-SE	基本要求： 以终端管理为核心，形成主机监控审计、补丁管理、桌面应用管理、信息安全管理、终端行为管控等终端安全行为一体的管理系统。配置400个PC许可；3年软件升级服务； 通用指标： 支持B/S模式管理，支持管理员三权分立。 支持SSL加密模式访问 服务器可以支持64位windows Server 2008/2012操作系统。 数据库支持Oracle10G/11G。 客户端可以支持windows XP、32位及64位win7/8/8.1操作系统。 WSUS补丁服务器支持2.0及以上。 资产管理： 类型配置查询：可查询资产的类型、品牌名称、型号名称、配置等信息，查询条件包括：资产类型、型号、品牌。 支持在线时长监控查询，显示终端在线累积时长、离线累积时长、最近下线时间、总时长等信息。 用户端管控： 运行监控中可以查看已登记、未登记在线终端的相关信息，包括：名称、类型、IP/MAC、版本、上线历史、漏洞、资产关联、验证情况等。 策略监控： 策略可根据风险等级进行告警，能够定义策略优先等级、策略生效时间、显示策略创建修改的人员及时间记录。 支持文件操作审计，可审计源文件名、用户、IP、时间、跟踪方向、跟踪操作、目标文件名、操作详情等信息。 系统管理：支持服务器监控管理，可监控本系统各模块服务运行状态。 服务： 提供原厂3年软件升级服务，提供原厂工程师3年上门服务，提供400个终端替换原有防护软件安装部署服务。	1	中国	3年

7	MCU 多点控制单元（内置会管平台）	华为 ViewPoint 9800-T	基本要求： 采用国产自主的编解码芯片和操作系统。 支持 ITU-T H.263、H.264BP、H.264HP、 H.265、H.264 SVC、H.265 SVC、H.265 SCC 等视频协议，支持 G.711、G.722、G.722.1C、G.729、AAC-LD、Opus、iLBC 等音频协议。 支持 4K30fps、1080p60fps、1080p30fps、720p60fps、720p30fps、4CIF 等视频格式。 支持 G.711、G.722、G.722.1C、G.729、AAC-LD、Opus、iLBC 等音频协议。 支持 AVC/SVC 混合会议，以适应不同线路带宽、不同设备能力、不同网络环境下的组网要求。 可靠性要求： 支持全编全解技术，确保每个接入的会场均能以任意不同的协议、带宽、格式、帧率参加同一组会议，会议中任何一个参会终端出现丢包仅影响该会场，不会影响整个会议效果。 多画面功能要求： 支持会议中每个会场观看独立的多画面，每个会场的多画面模式及多画面中所有分屏会场可设置，可设置 25 多画面。 双流指标： 支持辅流适配功能，辅流适配时不占用主流的资源。 网络适应性要求： 支持 40%网络丢包下，语音清晰连续，视频清晰流畅，无卡顿、无马赛克；支持 80%网络丢包下，声音清晰，不影响会议正常进行。 支持 IPv4 和 IPv6 双协议栈工作。 会议功能要求： 支持断线重呼功能，MCU 可自动重邀掉线或断电的终端再次入会。 安全性要求： 支持 SM2、SM3、SM4 国密加密算法，在全编全解会议模式下启用国密加密，MCU 接入端口容量不受影响。支持 SIP(TLS/SRTP)信令和媒体流加密、AES 加密算法、H.235 媒体流加密、H.235 认证和信令完整性校验。 支持口令复杂度提示和检测机制，口令长度至少 8 位，应包含数字、大小写字母、标点和特殊字符中至少 2 类。 支持对外管理接口(Web、SSH、SNMP、FTP)采用 https、sshv2、SNMPv3、ftps 安全加密传输方式，支持 Web、SSH 等远程管理服务，支持特定 IP 地址访问控制。 服务：原厂 5 年质保服务	1	中国	5 年

8	分体式高清会议终端	华为CloudLink BOX610	基本要求： 为保证系统兼容性，高清会议终端须与MCU同一品牌。 终端采用分体式结构，嵌入式操作系统，非PC、非工控机架构。 终端操作系统及编解码处理芯片为国产自主。 终端主要元器件须国产自主，至少包括视音频编解码单元、CPU处理单元、可编程逻辑芯片、电源模块、时钟芯片、视频输入输出芯片等。 支持ITU-T H.323和IETF SIP通信标准。支持H.263、H.264BP、H.264HP、H.265视频编解码协议；支持G.711、G.722、G.722.1C、G.729A、AAC-LD、Opus等音频协议。 支持64Kbps-8Mbps呼叫带宽，支持IPv4和IPv6网络协议。 支持4K30fps、1080p60fps、1080p30fps、720p60 fps、720p30fps等分辨率。本次项目配置1080P30fps对称编解码能力。 双流指标： 支持ITU-T H.239和IETF BFCP双流协议。 支持主流达到4K30fps情况下，辅流同时达到4K30fps。 接口要求： 支持4路高清视频输入接口、3路高清视频输出接口。 支持4路独立音频输入接口、4路独立音频输出接口，至少具备卡侬头、RCA等音频接口。 网络适应性要求： 支持在终端前面板显示启动、升级、休眠、异常信息、IP地址、H.323号码、SIP号码等信息。 触控终端： 配置触控平板，触控屏尺寸10英寸，支持终端休眠和唤醒、设置/取消静音、音量调节、摄像机PTZ控制、预置位设置及调用、双流共享、呼叫/挂断会场、添加/删除会场、观看/广播会场、结束会议、申请及释放主席等功能。 安全要求： 支持以硬件安全信任根为基础，以安全信任链校验机制对启动加载软件、操作系统和应用程序逐级安全校验，完全通过证书校验后方可启动终端。 服务：原厂5年质保服务	1	中国	5年
9	高清摄像机	华为CloudLink Camera 200	基本要求： 与所投高清会议终端为同一品牌，支持851万像素1/2.5英寸CMOS成像芯片，支持WDR图像数字宽动态功能。 支持1080p60、1080p30等视频输出格式。 支持12倍光学变焦。 支持水平视角80°。 水平转动范围：+/-110°，垂直转动范围：+/- 30°。	1	中国	5年

			支持 255 个预置位。 接口要求： 支持 2 路高清视频输出接口。 支持 2 个 RS-232 控制接口，支持标准 VISCA 控制协议。 功能要求： 支持自动白平衡（AWB）、自动曝光（AE）、自动聚焦（AF）功能。 支持图像倒转功能，方便摄像机安装在天花板上。 服务： 原厂 5 年质保服务			
10	全向麦克风	华为 CloudLink Mic 500	拾音距离： 数字阵列麦克风，支持 360° 全向拾音，拾音距离 6 米。 供电要求： 支持终端供电，不需要额外电源。 功能要求： 支持回声抵消、自动增益控制、自动噪声抑制。 采样率： 采样率 48KHz。 频响范围： 100Hz~22KHz。 服务：原厂 5 年质保服务	1	中国	5 年

甲方：

乙方：

法定代表人或授权代表：

法定代表人或授权代表：

签订日期：2024 年 8 月 2 日