**采购需求**

**一、采购标的**

|  |  |  |
| --- | --- | --- |
| **包号** | **采购内容** | **数量** |
| 02 | 云资源及网络安全服务项目 | 1项 |

**二、商务要求**

1.实施的期限和地点

1.1采购项目（标的）实施的时间：建设周期3个月之内，服务周期为自建设完成投入使用起3年。

1.2采购项目（标的）实施的地点：北京市门头沟区卫生健康委员会指定地点

2.付款条件（进度和方式）

详见“拟签订的合同文本”。

**三、技术要求**

1.基本要求

1.1采购标的需实现的功能或者目标

本次招标采购是为北京市门头沟区卫生健康委员会提供信息化平台建设相关服务，供应商应根据招标文件所提出的技术规格和服务要求以先进的技术、优良的服务和优惠的价格，充分显示自己的竞争实力。

1.2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

供应商应保证所提供的服务符合国家相关法律法规的要求。

2.验收标准

2.1符合采购人服务范围要求。

2.2供应商配置的硬件设备符合采购人要求。

2.3完成采购人要求的工作内容。

2.4达到采购人要求的服务和质量标准。

3.服务内容及要求/货物技术要求

3.1采购标的需满足的性能、材料、结构、外观、质量、安全、技术规格、物理特性等要求

详见其他技术、服务等要求

3.2采购标的需满足的服务标准、期限、效率等要求

详见其他技术、服务等要求

3.3为落实政府采购政策需满足的要求**（专门面向中小企业采购或预留份额的情况不享受政策优惠扣除）**

1）促进中小企业发展政策：根据《政府采购促进中小企业发展管理办法》的通知（财库〔2020〕46号）规定，本项目供应商所投产品为中小企业制造或提供服务由中小企业承接的，**供应商应出具招标文件要求的《中小企业声明函》给予证明，否则评标时不予认可**。**供应商应对提交的中小企业声明函的真实性负责，**提交的中小企业声明函不真实的，应承担相应的法律责任。

2）监狱企业扶持政策：供应商如为监狱企业将视同为小型或微型企业，应提供由省级以上监狱管理局、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。供应商应对提交的属于监狱企业的证明文件的真实性负责，提交的监狱企业的证明文件不真实的，应承担相应的法律责任。

3）促进残疾人就业政府采购政策：根据《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定，符合条件的残疾人福利性单位在参加本项目政府采购活动时，供应商应出具招标文件要求的《残疾人福利性单位声明函》，并对声明的真实性承担法律责任。中标、成交供应商为残疾人福利性单位的，采购代理机构将随中标结果同时公告其《残疾人福利性单位声明函》，接受社会监督。残疾人福利性单位视同小型、微型企业。不重复享受政策。

4）鼓励节能、环保政策：依据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知（财库（2019）9号）》执行。

3.4采购标的的其他技术、服务等要求

本包旨在通过采购服务，满足对招标人现有所有业务系统进行迁移与整合的资源支撑及安全保障，最终搭建一套基于C86架构的信创超融合资源池，用于稳定承载所有业务系统，并提供专线接入服务，将资源池与各需求单位进行打通，实现业务系统统一部署，集中管控，集中访问。投标人需具备丰富经验与专业能力，确保项目顺利实施，满足招标人业务发展的信息化需求。

**一、物理环境**

1.2机房需求

1. 提供放置设备（包括网络设备、安全设备、服务器等）所需的≥500平米的独立空间的标准机房环境，提供云资源设备所需的标准网络环境，集中放置、管理机柜。

（2）机房电缆总线输入应不低于 双路2000Kva市电引入标准，并配备UPS配电柜、发电车等，确保机房供电稳定性。

每个机柜提供双路PDU进行供电，单柜配备≥16A，总功率不低于6kW，且可根据业务需求，对供电指标进行相应扩容。

（3）机房应配备完善的消防系统，部署烟感、喷淋系统，并具备干粉、气灭、水浸等多种灭火手段，同时需具备防水、防涝措施。

（4）机房需部署精密空调，满足设备运行所需的温湿度环境。

（5）机房具备安全实时监控的视频图像数字信号，对机房环境进行全方位监控覆盖，并具备相应的安防措施及安全管理手段。

（6）为配合业务系统评定国家信息安全等级保护三级认证，机房标准需满足三级等保要求物理环境的要求。

（7）实行7\*24小时专人值守制度，以保证云资源系统的正常运行和专线链路的畅通，并重点保障重大活动期间及国庆、春节等国家法定节假日期间业务的连续。

**二、专线需求**

2.1专线资源需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 专线类型 | 带宽需求 | 固定IP需求 | 专线数量 |
| 1 | 互联网专线 | ≥100M | ≥16个 | ≥1条 |
| 2 | 政务网专线 | ≥100M | / | ≥1条 |
| 3 | 卫生网专线 | ≥1000M | / | ≥1条 |

2.2专线指标需求

（1）通信链路采用点到点独立通道，在传输过程中，专网传输平台不对所传输的数据做任何处理，完全实现了数据在网络中透明、安全的传输,网内所有设备专网专用，与其他网络物理隔离。

（2）具备自云平台至门头沟区各卫生点位专线敷设能力。

（3）线路质量与维护：专线应具备高质量的线路稳定性，投标人需提供 7×24 小时的线路监测与维护服务，服务团队不少于4人，可及时处理线路故障，保障专线通信质量。故障响应时间不超过10分钟，故障修复时间不超过2小时。

（4）可管理性：采用先进专用的网管系统，全程全网管理模式，能及时监视全网的运行状况，网管采用7\*24小时值班制度，随时有较强的技术力量支持，当网络出现故障时，网管可实施直接的垂直指挥调度，跨越环节少、反应时间短、解决问题快。

**三、资源需求**

3.1业务系统资源需求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 业务系统名称 | CPU资源（核） | 内存资源（G） | 存储资源（TB） | 备注 |
| 1 | 业务系统A | 96 | 128 | 8 |  |
| 2 | 业务系统B | 96 | 256 | 8 |  |
| 3 | 业务系统C | 96 | 256 | 8 |  |
| 4 | 数据库A | 96 | 256 | 32 |  |
| 5 | 数据库B | 96 | 512 | 32 |  |
| 6 | 数据库C | 96 | 512 | 56 |  |
| 合计： |  | 576 | 1800 | 144 |  |

（1）计算资源需求

要求投标人提供Vcpu\*600以及1800 GB内存的计算资源，以满足业务系统的计算资源需求。资源池物理节点不少于3个，节点配置为海光4代系列CPU，每节点配备2个CPU，每个CPU主频不低于2.5Ghz，核心数不少于32个，内存不少于640GB，确保计算资源的高效性与可靠性。

（2）存储资源需求

要求投标人提供不少于144TB的存储裸容量，底层采用分布式存储架构，支持多副本数据冗余技术，保障数据安全存储，存储读写性能满足业务系统并发访问需求。

（3）国产化需求

为满足国产化业务需求，云平台需要支持部署中标麒麟、银河麒麟、麒麟信安、深度Linux、统信UOS、openEuler、Anolis等国产化操作系统。

另外所投设备CPU等核心部件，需在中国信息安全评测中心认证目录，并可查询相关信息。https://www.itsec.gov.cn/

**四．服务需求**

**4.1服务需求**

为确保招标人业务系统顺利迁移、稳定安全运行，投标人需提供以下服务：

|  |  |  |
| --- | --- | --- |
| **序号** | **服务名称** | **服务内容** |
| 1 | 等保服务 | 需满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）第三级系统所对应的关键设备和节点冗余要求，投标人需提供承诺函并加盖公章。 |
| 2 | 系统整合服务 | 为了满足招标人需求，投标人需将招标人现有安全产品与安全架构相结合，提供定制化的安全服务。这包括但不限于对现有安全产品的评估、优化和整合，确保它们能够无缝地协同工作，以提供更加强大和全面的安全防护。 |
| 3 | 云互联网出口边界防护服务 | 需提供服务工具，对云互联网出口进行安全防护，对云互联网出口的流量进行监控、过滤和阻断，有效防止外部攻击和恶意软件的入侵。服务应包含但不限于DDoS攻击防护、入侵防御、恶意代码防范、策略分析、防勒索、防扫描等功能确保云互联网出口的稳定性和安全性。 |
| 4 | 端点安全服务 | 需通过工具对云主机实施全面的端点安全防护措施，包括主机漏洞扫描、补丁修复管理、终端基线检查、资产盘点、资产主动发现、轻补丁漏洞免疫以及弱密码检测等，以确保云主机的安全性。 |
| 5 | 日志审计服务 | 需通过日志审计工具对招标人云上系统相关云资产进行日志审计，提供一站式采集、加工、查询与分析、可视化与告警等功能，并满足日志留存合规要求。 |
| 6 | 数据库审计服务 | 需通过数据库审计工具，在满足等保2.0安全审计相关要求的同时，智能解析云数据库通信流量，细粒度审计数据库访问行为，通过对数据库全量行为的审计溯源、危险攻击的实时告警、风险语句的智能预警，提供敏感的数据库资产安全的监控保障。 |
| 7 | 安全运营服务 | 需通过提供服务工具，收集操作系统、网络产品、安全产品等基础设施的原始安全数据，对业务系统的网络安全情况进行分析，对分析结果进行整体、分段的展示，提升安全运营能力。 |
| 8 | 运维审计服务 | 需通过服务工具构建统一运维管理通道，集中管理资产权限，并支持分级分权管理，全程监控操作行为，实时还原运维场景，保障云端运维身份可鉴别、权限可管控、风险可阻断、操作可审计，助力等保合规。 |
| 9 | 边界隔离防护服务 | 需提供服务工具，对招标人接入云平台的接入区域边界进行安全防护，对边界出口的流量进行监控、过滤和阻断，有效防止外部攻击和恶意软件的入侵。服务应包含但不限于DDoS攻击防护、入侵防御、恶意代码防范、策略分析等功能，确保接入边界的稳定性和安全性。 |
| 10 | 定级备案服务 | 需基于招标人信息系统现状，参照《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020），对系统现状进行调研，根据调研结果，确定定级对象，分析定级要素，根据等级保护对象受到破坏时所侵害的客体和对客体造成的侵害程度确定系统等级，编制定级报告并协助备案。 |
| 11 | 脆弱性检测服务 | 需指派专业技术服务团队在招标人相关负责人现场监督下，对招标人信息系统通过手工脆弱性检查和使用漏洞扫描工具方式分别进行全面深入的脆弱性检测，全面深入地对网络及安全、主机、数据库等存在的各种技术漏洞进行检查，为安全加固提供客观依据，减少信息安全隐患，提高网络和系统安全防护能力。 |
| 12 | 安全加固服务 | 需根据脆弱性检测等工作结果，结合招标人信息系统业务需求，通过技术手段对信息系统相关的操作系统、数据库、中间件、网络与安全设备进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
| 13 | 网络安全管理制度修订服务 | 需基于信息系统安全等级，根据网络安全等级保护管理要求，从网络安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面对现有网络安全管理制度进行优化和修订，达到国家网络安全等级保护管理要求。 |
| 14 | 辅助测评服务 | 需针对信息系统等级保护测评提供咨询服务，协助通过等级保护测评，咨询服务内容包括系统现状调研，根据调研结果编制测评申请书，在测评现场提供技术支持，根据测评结果协助整改并提供复测咨询等。 |
| 15 | 三级等保测评 | 需依据国家相关政策文件要求，聘请具备信息安全等级保护测评资质的第三方测评机构对系统进行等级保护测评，检验系统是否符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的等级保护相关级别要求，了解网络安全等级保护要求在系统中的实施配置情况以及整体安全性，对系统的安全保障状况进行符合性安全测试和评估，评价系统是否满足安全等级测评要求中的各项安全。 |
| 16 | 应急演练服务 | 需结合招标人实际需求，为其提供定制化的应急演练服务，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。 |
| 17 | 安全培训服务 | 需为招标人提供形式多样的宣教培训，提升员工网络安全意识，增强网络安全素养，提高风险辨识和防范技能，建立网络安全的第一道防线。 |
| 18 | 产品质保服务 | 服务期内，要求投标人提供硬件设备故障返厂维修服务，维修期间需提供同型号、性能备品备件，维持业务正常运转。 |
| 19 | 软件升级服务 | 在服务期内，要求投标人提供软件升级服务，在确保软件系统稳定、安全的基础上具备最新的功能与安全特性。并在升级前向用户提供详细的升级方案与风险评估报告。 |
| 20 | 业务迁移服务 | 投标人需配合应用厂商制定全面的业务系统迁移方案，在迁移前对招标人现有业务系统进行评估，配合应用厂商完成业务系统迁移。 |
| 21 | 售后支持服务 | 投标人提供产品及软件相关技术问题的受理与处置、告警威胁相关问题的咨询与处理、硬件维修相关问题的服务，以及提供包含产品功能、使用配置等方面的服务咨询与解答服务。 |
| 22 | 服务周期要求 | 投标人需具备连续、长时间、稳定的服务支撑能力，并提供稳定、可靠的服务团队，服务周期的能力需≥3年。 |
| 23 | 运维服务 | （1）软件升级，包括：主线版本/R版本/SP版本等在线升级和定期补丁更新； （2）7\*24H风险在线监控，包括：服务器硬件健康状态监控、云平台运行状态监控、硬盘/内存亚健康风险提前预测，支持7\*24H持续在线监测； （3）7\*24H告警通知，支持小程序/短信/邮件/语音/企微/钉钉/飞书等多种方式告警通知； （4）支持智能根因分析、影响面评估，支持拓扑图形式呈现故障根因链路，并提供合理的处置建议，以提升问题排障和处置效率； （5）支持生成运维报告，包括平台服务器健康风险预测和评估（如：CPU/内存/硬盘/Raid卡/网卡等）、云主机运行状态（如：CPU/内存/网络等）风险评估等； （6）安排专属客户经理1名，受理甲方日常运维、业务改造等需求对接，及时响应客户需求。 |

**4.2云资源技术参数**

“★”标识项为关键指标项，不满足将导致投标无效。

注：

1、投标人须如实提供技术指标要求的证明材料，证明材料可以使用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。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、产品供货后，采购人将对中标产品进行性能测试和功能验证，与投标承诺不符将做为无效投标处理，由此引发的所有损失由该投标人承担。

|  |  |
| --- | --- |
| **服务指标项** | **服务指标要求** |
| 总体要求 | 1.要求所投超融合产品的计算虚拟化软件类、存储虚拟化软件类、网络虚拟化软件类为同一品牌且完全自主研发，提供相应的计算机软件著作权登记证书。 |
| 2.采用裸金属架构，无需绑定操作系统即可搭建超融合平台。 |
| 节点配置 | ★规格2U，配置2颗国产C86架构CPU，主频≥ 2.5GHz，核心数≥32，内存配置≥10\*64GB DDR5 5600Mhz，系统盘配置≥2\*480GB SATA SSD，缓存盘配置≥2\*3.84TB NVMe SSD，数据盘配置≥6\*8TB HDD，配置冗余电源，接口配置≥4个千兆电口，4个万兆光口； |
| 2.软硬件均支持ECC告警。支持提前发现内存CE故障，并且实现100%异常自动隔离。支持内存UE故障检测告警，并在用户界面显示告警信息。 |
| 计算虚拟化软件 | ★1.配置并激活计算虚拟化软件，每个节点配置2颗CPU计算虚拟化软件授权。 |
| 2.考虑医院实际运维需求，要求当虚拟机卡死或蓝屏时虚拟机需具备自动检测功能并实现自动重启，无需人工干预，减少运维工作量。 |
| 3.为保证业务运行可靠性，要求支持IO重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。 |
| 4.提供基于PowerShell的CLI命令行功能，通过命令行可以进行管理计算虚拟化、存储虚拟化、网络虚拟化模块，并通过PowerShell脚本可简化用户运维操作。支持漏洞及版本信息巡检，推送补丁及升级信息，并支持补丁管理、更新、回滚。（提供产品功能截图/证明材料并加盖公章） |
| 5.虚拟化管理平台具备监控功能，对资源池中CPU、网络、磁盘使用率等指标进行实时的数据统计，当指标超过设置的阈值，可以通过多种方式（短信、邮箱）告知管理员进行排障。 |
| 6.为充分利用云平台的资源，虚拟机需要支持内存回收，在内存不用的时候自动回收给其他虚拟机使用，并支持手动设置平台的内存超配比例，实现内存的超分使用。 |
| ▲7.部分业务需要使用USB设备，需支持物理机上的USB映射给虚拟机使用，且虚拟机迁移或故障迁移到其他主机上也能自动映射USB设备。（提供带有CMA或CNAS标识的检测报告证明并加盖公章） |
| 存储虚拟化软件 | ★1.配置并激活存储虚拟化软件，每个节点配置2颗CPU存储虚拟化软件授权。 |
| 2.支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。 |
| 3.硬件故障对平台影响较大，也会影响数据安全，为保障核心业务在硬件故障后尽快恢复冗余数据保障，重建过程中可以查看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等；支持点击操作中的优先级对数据重建进行优先重建（提供带有CMA或CNAS标识的检测报告证明并加盖公章） |
| 4.支持iSCSI存储、FC存储、NFS存储、本地存储。支持通过iSCSI透传/非透传指令使虚拟机支持存储裸设备映射（RDM），可以将存储设备上的LUN 直接映射给虚拟机使用。 |
| ▲5.支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达30min/TB以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性。（提供带有CMA或CNAS标识的检测报告证明，并加盖公章） |
| 6.为保证亚健康硬盘的数据安全，支持主动将亚健康硬盘数据进行迁移修复，当硬盘的坏 道数过多，系统能够自动将该盘的数据迁移至其他健康硬盘上。（提供带有CMA、CNAS标识的检测报告证明，并加盖公章） |
| 网络虚拟化软件 | ★1.配置并激活网络虚拟化软件，软件按照物理CPU数量方式进行授权，每个节点配置2颗CPU网络虚拟化软件授权。 |
| 2.在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率。 |
| 3.分布式防火墙基于监测虚机IP地址和端口进行东西向流量隔离控制，并提供实时拦截日志，以及支持“数据直通ByPass”功能，方便出现问题快速定位问题。 |
| ▲4.无需单独购买授权，超融合自带分布式防火墙功能，并支持微隔离策略推荐，自动通过访问关系、历史流量和用户配置来生成最适合的微隔离规则，并且可以预发布策略，预览访问关系和防护状况，在二次确认后发布推荐策略。（提供带有CMA、CNAS标识的检测报告证明并加盖公章） |
| 系统迁移 | ▲提供同品牌自研的迁移工具，无需采购第三方迁移服务，支持原主机和异构目标机之间的自动化迁移功能。（提供产品功能截图/证明材料并加盖公章） |

**4.3安全服务技术参数**

**4.3.1 云互联网出口边界防护服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 云互联网出口边界防护服务 | 1.网络层吞吐量≥20G，并发连接数≥300万，新建连接数≥9万 |
| 2.需支持不少于16000种漏洞规则，支持展示漏洞ID、名称、危险等级、漏洞CVE标识、漏洞描述等特征信息。 |
| 3.需支持分析安全策略是否冗余、当前策略匹配情况，当前策略是否遗漏风险端口等维度分析并支持针对分析结果提供优化建议。 |
| ▲4.需支持独立的勒索病毒防护模块，非普通防病毒功能，支持进行勒索风险自动化评估，并依据评估结果自动生成防护策略。（提供产品功能截图及关于“勒索病毒”的软件著作权证明功能有效性并加盖公章） |
| 5.需支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护。 |
| 6.需支持服务器漏洞专项防扫描功能，针对扫描设备的IP地址能够及时发现并阻断。 |
| 7.需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。 |
| 8.需具备URL分类库，支持管控非法、违规网站的访问行为。 |
| 9.需支持对Teardrop攻击、Smurf攻击、Land攻击等异常数据包的检测和防御。 |
| 10.需支持超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（提供产品功能截图及具备CMA/CNAS标识的第三方检测报告并加盖公章） |
| 11.需支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息。 |
| 12.需支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换选路模式支持智能负载选路、按指定顺序选路、优先使用质量最优的线路、按剩余带宽比例负载。 |
| 13.需支持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。 |
| 14.需支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。 |
| ▲15.为保障工具的可靠性和生产商的技术开发能力，要求服务工具厂商提供《CCRC 信息安全服务-软件开发服务资质》一级证书。（提供有效证书扫描件并加盖公章） |

**4.3.2 端点安全服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 端点安全  服务 | 1.需包含≥60点授权。 |
| 2.需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，包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。 |
| 3.需支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组。 |
| 4.需支持禁止黑客工具启动，包含：xuetr、ProcessHacker、PCHunter、Mimikatz等工具的自启动，可以防止黑客攻击；（提供产品功能截图并加盖公章） |
| 5.需支持安全策略一体化配置，通过单一策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell检测和威胁处置方式、暴力破解的威胁处置方式和Windows白名单信任目录。 |
| 6.需支持以可视化形式展现攻击故事，提供可视化的进程树溯源，可直观看出攻击入口、相关操作行为、高危实体文件等信息，协助进行事件攻击溯源和研判分析。 |
| 7.需支持一键式操作对指定Linux终端/终端组进行通用安全检查基线、等保二级基线、等保三级基线、CIS系统基线、CIS应用基线、以及基于以上基线规则原型的自定义基线的合规性检查，可视化展示终端的基线合规检查结果，并对不合规的检查项提供设置建议。 |
| 8.需支持全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置。 |
| 9.需支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括SSH、RDP、MySQL、Tomcat、Redis等应用类型，可按照空密码、自定义弱密码、密码长度小于8、字符种类小于3等常见弱密码类型进行分类查看。 |
| 10.需支持按照扫描网段、扫描方式、扫描协议、扫描端口对终端进行扫描，及时发现尚未纳入管控的终端 |
| 11.需支持流行Windows高危漏洞的轻补丁免疫防御，支持Windows补丁批量一键修复 |
| ▲12.需支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵；需支持Linux服务器SSH远程登录保护，可开启SSH远程登录二次认证，以防止黑客利用弱密码脆弱性对服务器的入侵；支持设置验证码验证或自定义密码验证，支持设置登录认证提示、生效时间段和免二次认证白名单；  （提供产品功能截图并加盖公章） |
| 13.需支持一键式操作对指定Windows终端/终端组进行通用安全检查基线、等保二级基线、等保三级基线、CIS系统基线、CIS应用基线、以及基于以上基线规则原型的自定义基线的合规性检查，可视化展示终端的基线合规检查结果，并对不合规的检查项提供设置建议 |
| ▲14.需支持基于威胁情报的病毒文件哈希值、行为、域名、网络连接等各项终端系统层、应用层行为数据在全网终端发起搜索，挖掘潜伏攻击，快速定位出全网终端感染该威胁的情况（提供产品功能截图并加盖公章） |
| 15.需支持自定义Linux、Windows系统深度防护加固策略，包含禁止对外服务进程编译文件 、禁止对外服务进程创建危险的定时任务脚本、禁止非系统进程尝试劫持EXE执行过程、禁止对外服务进程添加定时任务等。 |
| 16.需采用SSVC决策树的模优先级排序模型，结合漏洞自身属性、外部漏洞情报以及资产暴露面等多个维度，在现有CVSS漏洞评分的基础上进一步消减高危漏洞数量，对发现的漏洞进行优先级排序，包含响应、关注、观察3种结果，辅助用户快速聚焦应该优先关注的漏洞威胁。 |

**4.3.3 日志审计服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 日志审计服务 | 1.需支持包含≥300个资产授权； |
| 2.需支持资产数据总览，统计展示监控资产总数、历史接收日志总数、事件总数及占比情况、资产风险度； |
| 3.需支持数据接收通道状态展示，可查看系统当前接收日志数据通道的负载能力； |
| 4.需支持事件数据总览，统计展示历史事件总数、极危历史事件数、高危历史事件数和今日高危资产数；需支持今日高危资产列表的查看，包括资产IP、资产类型、极危事件数、高危事件数； |
| 5.需支持按字段进行事件查询，查询字段包括资产名称、资产IP、事件名称、事件级别、事件发生时间等不少于20个字段；支持多条件联合查询和查询条件的保存功能； |
| 6.需支持综合报表的配置与生成，支持配置报表的统计时间以及包括整体概述、日志分析、事件分析、资产分析等在内的统计内容，支持开启报表的对比模式，支持报表预览； |
| 7.需支持事件报表功能；支持按照系统内置事件和关联事件进行统计报表生成。 |
| 8.需支持日志动作管理功能，具备产品内置动作不少于2000条，内置动作信息包括动作分类、动作名称、动作描述、资产图标、动作类型；（提供产品功能截图并加盖公章） |
| 9.需具备告警事件库，支持内置事件和关联事件，页面支持展示事件分类、事件名称、事件描述、事件级别等信息； |
| 10.需支持事件告警设置，可针对不同类型的事件设置告警方式，支持弹窗告警、邮件告警、短信告警，支持设置告警的通知角色、通知频次； |
| 11.需支持用户名密码方式、证书方式、Radius方式等多因子认证功能； |
| 12.需支持采用SM4算法的日志数据加密存储和管理数据加密传输；（提供产品功能截图并加盖公章） |
| ▲13.需具备麒麟软件NeoCertify认证证书、统信软件产品互认证明；（提供有效证书扫描件并加盖公章） |

**4.3.4 数据库审计服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 数据库审计服务 | 1.十亿在线数据查询耗时需≤1秒，五十亿在线数据查询耗时需≤5秒，百亿在线数据查询耗时需≤10秒；支持数据库实例上限需≥16个。 |
| 2.需支持审计和告警语句会话回放。 |
| ▲3.审计日志导出控制，需要输入密码认证。（提供产品功能截图并加盖公章） |
| 4.需支持原始数据采集，对各种数据库的流量信息进行详情监测功能，包括数据库地址、进出记录的时间和风险信息等日志。 |
| 5.需支持风险批量处置。 |
| 6.需支持Syslog、Snmp Trap、邮件等三种告警方式功能。 |
| 7.需支持从多维度对日志数量、风险数量、SQL流量进行展示。 |
| 8.需支持对统计数据进行下钻分析、以列表方式展示分析结果。 |
| 9.需支持对象统计、可查看对象访问的详情，支持桑基图统计对象操作信息。 |
| 10.需支持三权分立，提供系统管理员、安全管理员、审计管理员，满足合规要求。 |
| ▲11.需具备软件著作权登记证书及网络安全专用产品安全检测证书；需具有中国网络安全审查认证和市场监管大数据中心（原中国网络安全审查技术与认证中心）颁发的中国国家信息安全认证证书；  （提供有效证书扫描件并加盖公章） |
| ▲12.需具有麒麟软件适配认证证书；（提供证书复印件并加盖公章） |

**4.3.5 安全运营服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 安全运营服务 | 1.需支持管理≥300个资产。 |
| 2.需展示平台综合态势；支持展示资产总体安全态势及资产安全指数、告警、统计；展示漏洞闭环处置数量情况，漏洞数量趋势图；支持展示安全告警数量及趋势图；支持展示威胁事件的数量情况，以态势图及趋势图两种不同形式展示威胁分类和数量；支持对工单的响应处置进行统计。 |
| 3.需展示资产的运营状态页面；支持展示不同状态资产的数量以及资产中检测到的不同类型告警数量、威胁事件数量、监控状态数量；统计展示风险指数最高的资产/业务系统排行、资产安全趋势图、外连威胁列表；支持展示资产检测到的实时告警列表，并可通过列表内点击跳转至漏洞处置页面。（提供产品功能截图并加盖公章） |
| 4.需支持资产台账的展示；统计展示各类型资产数量及总数、资产类型树、资产列表；需支持对资产的查询、添加、导入、导出、修改、删除、配置等操作。 |
| 5.需展示拓扑管理页面；页面内展示可选择绘制的资产类型及连线，需展示拓扑图以反映组网情况和运行状态；支持拓扑图的绘制、添加及删除连线、节点的添加及删除等操作。 |
| 6.需展示概览统计页面；页面需展示日志数量统计、今日日志数据类型统计图、近30天日志数量趋势图、近15天日志告警趋势图。 |
| 7.需展示实时告警页面；页面需展示今日告警数、已处置告警数、未处置告警数、告警总量；需支持统计展示近15天的告警数量趋势图；需支持展示未处置告警列表、已处置告警列表、已忽略告警列表；需支持对未处置告警生成工单、批量忽略、详情查看等操作；已处置告警列表需支持详情查看操作，详情信息需包括告警信息、规则详情、告警数据源、资产信息。 |
| 8.需展示合规风险页面；页面需展示配置不合规项、巡检风险项、资产发现风险项。 |
| 9.需展示性能告警页面；页面需展示性能告警列表，列表信息包括但不限于告警名称、级别、资产名称、阈值、实际值、告警开始时间、告警恢复时间、告警次数、告警状态；支持对监控告警详情进行查看。 |
| 10.需展示资产监控页面，页面需展示资产数量、开启监控数量、未开启监控数量、资产异常数量、资产中断数量、资产卡片/列表等。 |
| 11.需展示拓扑监控页面；页面需展示资产数量、开启监控数量、未开启监控数量、资产异常数量、资产中断数量、拓扑图、资产卡片、实时监控告警。 |
| 12.需展示配置核查报告页面；页面需展示配置核查报告任务列表及生成周期报告任务列表；需支持生成单次配置核查报告及周期配置核查报告；13.需支持报告的详情查看、删除、再次生成、下载操作；报告详情需展示报告综述、资产详情、检查项详情、参考标准。 |
| 14.需展示安全运营报告页面；页面需展示安全运营报告任务列表及生成周期报告任务列表；需支持生成单次安全运营报告及周期安全运营报告；需支持报告的详情查看、删除、再次生成、下载操作； |
| 15.需支持对登录日志及操作日志的管理。 |
| ▲16.需具备麒麟软件NeoCertify认证证书、统信软件产品互认证明；（提供有效证书扫描件并加盖公章） |
| ▲17.在服务期间，投标方须派遣1名服务工具供应商的原厂技术专家，为招标人信息系统提供1次安全巡检服务，服务人员需具备信息安全工程师、网络工程师、信息系统项目管理师证书，需提供证书复印件并加盖公章。 |

**4.3.6 运维审计服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 运维审计服务 | 1.系统需包含≥300个授权； |
| 2.需支持对资源及登录账户进行管理功能，包括新增、查询、修改、批量导入、导出、删除、分组等操作；需支持主机资源通过IP地址和端口号进行自动发现功能； |
| 3.需支持对资产账户验证功能，可设置连接超时时间；任务完成后通过邮件、短信等方式通知； |
| ▲4.需支持用户USBkey签发功能，支持用户动态令牌签发和批量导入功能，并支持覆盖已有令牌；（提供产品功能截图并加盖公章） |
| 5.需支持对用户的批量导入功能，导入格式包括xls/xlsx/csv等；批量导入用户支持覆盖已有用户。 |
| 6.需支持访问控制类策略管理功能，访问控制策略内容包括访问时间、IP地址段、上传下载、文件管理、显示水印等内容；登录时间段需满足以周为单位，精确到小时级。 |
| 7.需支持资产配置备份策略管理功能，执行方式包括手动执行、定时执行和周期性执行；支持外部服务器存储；支持对单个账户和账户组进行配置备份； |
| 8.需支持对关键资源进行双人授权功能；（提供产品功能截图并加盖公章） |
| 9.需提供类主机网盘存储功能，支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计。 |
| 10.需支持快速运维管理功能，包括命令运维、脚本运维、文件传输等内容。 |
| ▲11.需满足密评要求，支持国产化算法SM2,可通过支持SM2算法的证书认证登录；需具有麒麟软件适配认证证书；（提供产品功能截图并加盖公章） |
| ▲12.需为运维人员提供10张个人数字证书，证书颁发机构需具备工信部颁发的《电子认证服务许可证》和国家密码管理局颁发的《电子政务电子认证服务机构》、《电子认证服务使用密码许可证》证明；若投标人不是依法设立的电子认证服务提供者的，还需要提供证书颁发机构给投标人出具的针对本项目的授权书。 |

**4.3.7边界隔离防护服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 边界隔离防护服务 | 1.需提供服务工具，对招标人接入云平台的接入区域（卫生网）边界进行安全防护，对边界出口的流量进行监控、过滤和阻断，有效防止外部攻击和恶意软件的入侵。服务应包含但不限于DDoS攻击防护、入侵防御、恶意代码防范、策略分析等功能，确保接入边界的稳定性和安全性。 |
| 2.需具备防病毒功能、入侵防御功能。 |
| 3.吞吐量需≥ 4G。 |

**4.3.8 定级备案服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 定级备案服务 | 1.服务内容：需基于招标人信息系统现状，参照《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020），对系统现状进行调研，根据调研结果，确定定级对象，分析定级要素，根据等级保护对象受到破坏时所侵害的客体和对客体造成的侵害程度确定系统等级，编制定级报告并协助备案。 |
| 2.服务范围：招标人指定的2个信息系统。 |
| 3.服务频次：服务期限内提供1次。 |
| 4.服务成果需包括但不限于：  《门头沟卫健委xx系统定级报告》  《门头沟卫健委xx系统备案证明》 |

**4.3.9脆弱性检测服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 脆弱性检测服务 | 1.服务内容：需指派专业技术服务团队在招标人相关负责人现场监督下，对招标人信息系统通过手工脆弱性检查和使用漏洞扫描工具方式分别进行全面深入的脆弱性检测，全面深入地对网络及安全、主机、数据库等存在的各种技术漏洞进行检查，为安全加固提供客观依据，减少信息安全隐患，提高网络和系统安全防护能力。 |
| 2.服务范围：招标人指定信息系统。 |
| 3.服务频次：服务期限内每年提供2次。 |
| 4.服务成果需包括但不限于：  《门头沟卫健委脆弱性检测报告》 |

**4.3.10安全加固 服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 安全加固服务 | 1.服务内容：需根据脆弱性检测等工作结果，结合招标人信息系统业务需求，通过技术手段对信息系统相关的操作系统、数据库、中间件、网络与安全设备进行安全策略加强、调优，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。 |
| 2.服务范围：招标人指定信息系统。 |
| 3.服务频次：服务期限内每年提供1次。 |
| 1. 服务成果需包括但不限于：   《门头沟卫健委安全加固报告》 |

**4.3.11网络安全管理制度修订服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 网络安全管理制度修订服务 | 1.服务内容：需基于信息系统安全等级，根据网络安全等级保护管理要求，从网络安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面对现有网络安全管理制度进行优化和修订，达到国家网络安全等级保护管理要求。 |
| 2.服务范围：招标人指定信息系统。 |
| 3.服务频次：服务期限内每年提供1次。 |
| 4.服务成果需包括但不限于：  《门头沟卫健委网络安全管理制度》 |

**4.3.12辅助测评服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 辅助测评服务 | 1.服务内容：需针对信息系统等级保护测评提供咨询服务，协助通过等级保护测评，咨询服务内容包括系统现状调研，根据调研结果编制测评申请书，在测评现场提供技术支持，根据测评结果协助整改并提供复测咨询等。 |
| 2.服务范围：招标人指定的2个信息系统。 |
| 3.服务频次：服务期限内每年提供1次。 |
| 4.服务成果需包括但不限于：  门头沟卫健委辅助测评过程文档 |

**4.3.13 三级等保测评**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 三级等保测评 | 1.服务内容：需依据国家相关政策文件要求，聘请具备信息安全等级保护测评资质的第三方测评机构对系统进行等级保护测评，检验系统是否符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）的等级保护相关级别要求，了解网络安全等级保护要求在系统中的实施配置情况以及整体安全性，对系统的安全保障状况进行符合性安全测试和评估，评价系统是否满足安全等级测评要求中的各项安全。 |
| 2.服务范围：招标人指定的2个信息系统。 |
| 3.服务频次：服务期限内每年提供1次。 |
| 4.服务成果需包括但不限于：  《门头沟卫健委xx信息系统等保测评报告》 |

**4.3.14应急演练服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 应急演练服务 | 1.服务内容：需结合招标人实际需求，为其提供定制化的应急演练服务，一方面使相关方熟悉应急响应流程，提高对安全事件的响应能力；另一方面验证预案正确性和适用性，进行总结分析，根据需要对应急预案进行修订。 |
| 2.服务范围：招标人指定的应急演练场景。 |
| 3.服务频次：服务期限内每年提供1次。 |
| 4.服务成果需包括但不限于：  《门头沟卫健委应急演练报告》 |

**4.3.15安全培训服务**

|  |  |
| --- | --- |
| **服务名称** | **服务指标要求** |
| 安全培训服务 | 1.服务内容：需为招标人提供形式多样的宣教培训，提升员工网络安全意识，增强网络安全素养，提高风险辨识和防范技能，建立网络安全的第一道防线；并根据客户需要提供相关指导服务。 |
| 2.服务要求：培训方式需包括但不限于移动端、网页端等，需提供截图证明材料； |
| ▲3.服务要求：该培训服务工具需具备近三年内为卫生健康行业提供同类网络安全培训的经验；需提供用户发布的培训通知或服务合同作为证明材料。 |
| 4.服务范围：招标人指定人员。 |
| 5.服务频次：服务期限内每年提供1次。 |
| 6.服务成果需包括但不限于：  安全培训记录 |

1. **村卫生室监控项目**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **（一）监控设备清单** | | | | | |
| **序号** | **商品名称** | **技术规格** | **单位** | **数量** | **备注** |
| 1 | 400万人脸文搜变焦网络摄像机 | 1.≥400万变焦筒型网络摄像机 2.最高分辨率可达2688 × 1520 @25 fps，在该分辨率下可输出实时图像 3.支持Smart侦测：场景变更侦测，虚焦侦测，区域入侵侦测，越界侦测，进入区域侦测，离开区域侦测，物品遗留侦测，物品拿取侦测，徘徊侦测，停车侦测，人员聚集侦测，快速移动侦测，音频异常侦测，音频陡升侦测，音频陡降侦测 4.支持背光补偿，强光抑制，3D数字降噪，120 dB宽动态 5.支持白光/红外双补光，红外光最远≥50 m，白光最远≥30 m 6.支持H.265/H.264/MJPEG视频压缩算法，支持多级别视频质量配置、编码复杂度设置 7.支持1路报警输入，1路报警输出（报警输出最大支持DC12 V，30 mA），1路音频输入，1路音频输出 8.支持最大512 GB MicroSD/MicroSDHC/MicroSDXC卡本地存储 9.1个内置麦克风 10.符合≥IP66防尘防水设计 11.传感器类型：1/3" Progressive Scan CMOS 最低照度：彩色：0.005 Lux  12.焦距&视场角：≥2.5~13mm，水平视场角：≥102°~31°，垂直视场角：≥54.5°~17.5°，13.对角视场角：≥122°~35.5°  14.补光灯类型：支持白光，红外补光 15.补光距离：红外光最远可达50 m，白光最远可达30 m 16.防补光过曝：支持 17.红外波长范围：≥850 nm  18.最大分辨率：≥2688 × 1520 19.视频压缩标准：主码流：H.265/H.264，支20.持超级智能编码 21.子码流：H.265/H.264/MJPEG 22.第三码流：H.265/H.264  23.宽动态：120 dB  24.网络：1个RJ45 10 M/100 M自适应以太网口 25.SD卡扩展：内置MicroSD/MicroSDHC/MicroSDXC插槽，最大支持512 GB 26.音频：1个内置麦克风 27.1路输入（Line in），最大输入幅值：3.3 Vpp，输入阻抗：4.7 kΩ，接口类型：非平衡 28.1路输出（Line out），最大输出幅值：3.3 Vpp，输出阻抗：100 Ω，接口类型：非平衡 29.报警：1路输入，1路输出（报警输出最大支持DC12 V，30 mA） 30.复位：支持 31.电源输出：DC12 V，100 mA，建议用于拾音器供电  32.产品尺寸：≥94 × 100 × 195 mm 33.包装尺寸：≥315 × 135 × 140 mm 34.设备重量：≤760 g 35.带包装重量：≤1050 g 36.启动和工作温湿度：-30 °C~60 °C，湿度小于95%（无凝结） 37.恢复出厂设置：支持RESET按键，客户端或浏览器恢复 38.电流及功耗：DC：12 V，0.63 A，最大功耗：7.5 W 39.PoE：IEEE 802.3af，CLASS 3，最大功耗：9 W 40.供电方式：DC：12 V ± 25% 41.PoE：IEEE 802.3af，CLASS 3 42.电源接口类型：Ø5.5 mm圆口  43.防护：IP66  **需提供厂商售后服务承诺函** | 台 | 178 |  |
| 2 | 摄像机支架 | 1.金属壁装支架 2.压铸纯铝合金材质，表面做喷塑处理 3.支架带出线孔，安装更加美观 4.摄像机安装座表面有海绵垫，保证和摄像机5.底座结合更紧密 6.摄像机安装座可旋转，方便摄像机角度调整 7.材质：铝合金 | 个 | 178 |  |
| 3 | 千兆交换机 | 1.支持10个10/100/1000M自适应电口，2个1G/2.5G SFP光口，固化单交流电源和风扇，1-8端口支持PoE/PoE+远程供电，125W POE供电 | 台 | 89 |  |
| 4 | 千兆交换机 | 支持24个10/100/1000Base-T自适应以太网接口，4个2.5G/1G SFP接口 | 台 | 9 |  |
| 5 | 网络硬盘录像机 | 1.2U机架式8盘位嵌入式网络硬盘录像机，采用短机箱设计，搭载高性能ATX电源 2.存储接口：8个SATA接口，可配备12TB硬盘 3.视频接口：2×HDMI，2×VGA 4.网络接口：2×RJ45 10/100/1000Mbps自适应以太网口 5.报警接口：16路报警输入，4路报警输出 6.串行接口：1路RS-232接口，2路半双工RS-485接口 7.USB接口：2×USB 2.0，1×USB 3.0 8.输入带宽：256Mbps 9.输出带宽：160Mbps 10.接入能力：32路H.264、H.265格式高清码流接入 11.解码能力：最大支持24×1080P 12.显示能力：最大支持4K+1080P异源输出 | 台 | 3 |  |
| 6 | AI 12TB | 片 | 35 |  |
| 7 | 网络硬盘录像机 | 1.2U机架式8盘位嵌入式网络硬盘录像机，采2.用短机箱设计，搭载高性能ATX电源 3.存储接口：8个SATA接口，可配备12TB硬盘 4.视频接口：2×HDMI，2×VGA 5.网络接口：2×RJ45 10/100/1000Mbps自适应以太网口 6.报警接口：16路报警输入，4路报警输出 7.串行接口：1路RS-232接口，1路全双工RS-485接口 8.USB接口：2×USB 2.0，2×USB 3.0 9.解码能力：最大支持16×1080P 10.显示能力：最大支持4K+1080P异源输出  **需提供厂商售后服务承诺函** | 台 | 1 |  |
| 8 | 网络硬盘录像机 | 1.5U机架式4盘位嵌入式网络硬盘录像机，采用短机箱设计，搭载高性能ATX电源 2.存储接口：4个SATA接口，可配备12TB硬盘 3.视频接口：2×HDMI，1×VGA 4.网络接口：2×RJ45 10/100/1000Mbps自适应以太网口 5.报警接口：16路报警输入，4路报警输出 6.串行接口：1路RS-232接口，2路半双工RS-485接口 7.USB接口：2×USB 2.0，1×USB 3.0 8.接入能力：16路H.264、H.265格式高清码流接入 9.解码能力：最大支持24×1080P 10.显示能力：最大支持4K+1080P异源输出  **需提供厂商售后服务承诺函** | 台 | 2 |  |
| 9 | 网络硬盘录像机 | 1.1U机架式2盘位嵌入式网络硬盘录像机，采用短机箱设计，搭载高性能电源 2.存储接口：2个SATA接口，可配备12TB硬盘 3.视频接口：1×HDMI，1×VGA 4.网络接口：2×RJ45 10/100/1000Mbps自适应以太网口 5.报警接口：4路报警输入，1路报警输出 6.USB接口：2×USB2.0 7.接入能力：8路H.264、H.265格式高清码流接入 8.解码能力：最大支持24×1080P 9.显示能力：最大支持4K+1080P异源输出  **需提供厂商售后服务承诺函** | 台 | 3 |  |
| 10 | 千兆交换机 | 三层交换机；≥28口SFP接口（SFP为千兆/百兆口），8个复用的10/100/1000M自适应电口，4个1G/10G SFP+光口，2个扩展槽，2个模块化电源插槽（含电源模块） | 台 | 1 |  |
| 11 | 流媒体服务器 | 1.2U 3000双路标准机架式服务器  2.CPU：配置2颗处理器，单处理器物理核心数≥8核，主频≥3.0 GHz，末级缓存容量≥16 MB，线程数≥16线程，热设计功耗≥90 W，支持内存的最高速率≥3200 MHz，通道数≥2，位宽≥64；  3.内存：配置64G DDR4，8根内存插槽，最大可支持扩展至1TB；  4.硬盘：2块600G 10K SAS硬盘（Raid1），前置最大可选支持12块3.5寸(兼容2.5寸)热插拔SATA/SAS硬盘，后置最大可选支持2块2.5寸热插拔SATA/SAS硬盘，内置最大可选支持2块2.5寸非热插拔SATA SSD硬盘，板载最大可选支持1个SATA M.2硬盘  3.阵列卡：配置SAS\_HBA卡（支持RAID 0/1/10）  PCIE扩展：最大支持4个标准PCIE插槽；  4.网口：配备板载2个千兆电口和2个PCIE千兆电口，可选配置2个万兆网口，支持选配10GbE SFP+等多种网络接口  5.其他接口：配备1个IPMI RJ-45管理接口，位于机箱后部；7个USB 3.0接口 4个位于机箱后部，2个位于机箱前部，1个位于机箱内部；2个VGA接口 1个位于机箱前部，1个位于机箱后部；  6.电源：配置550W（1+1）冗余电源  7.机箱规格：≥87.5mm(高)x 446.5mm(宽)x700mm(深) 不含箱耳  8.设备重量：≤23千克（含导轨） | 台 | 1 |  |
| 12 | 视频服务器 | 1.2U单路标准机架式服务器  2.CPU：配置1颗处理器，核数≥12核，主频≥2.4GHz  3.内存：配置64G DDR5，8根内存插槽，最大支持扩展至1TB内存  4.硬盘：配置2块1.2T 10K 2.5寸 SAS硬盘，默认支持8个3.5寸/2.5寸硬盘，配置最大支持12个3.5寸/2.5寸硬盘，配置兼容4个NVMe硬盘  5.阵列卡：配置SAS+HBA卡，支持RAID 0/1/10;  PCIE扩展：支持4个PCIe扩展插槽（包括1个OCP 插槽），其中2个PCIe 5.0  6.网口：板载2个千兆电口； 配置10GbE、25GbE SFP+等多种网络接口  7.其他接口：1个RJ45管理接口，后置2个USB 3.0接口，前置2个USB2.0接口，1个VGA接口  8.电源：配备550W（1+1）冗余电源  9.机箱规格：87mm(高)x 466mm(宽)x680mm(深) | 台 | 1 |  |
| 13 | 软件 | 1、提供门户首页内容自定义能力，支持自定义快捷入口、自定义菜单内容、自定义页面元素设置；支持门户展示元素自定义，包括页面logo图标、修改网站标题、设置并添加网站外部链接； 2、提供统一的认证、鉴权管理、应用管理、菜单管理、用户管理、角色管理、组织管理、资源管理等能力； 3、提供用户权限管理能力，包括菜单权限、组织权限、区域权限、资源权限、功能控制权限； 4、提供组织、区域、设备、人员、卡片、车辆等资源统一管理； 5、提供用户安全管理，支持账户绑定用户mac地址及IP地址能力，提供账户安全设置，支持账户密码有效期设置，支持登录类型（Web端、PC客户端、移动端）和认证方式（密码、PKI）的配置； 6、提供NTP校时服务能力，支持对设备和服务器统一校时; 7、提供数据、服务等统一开放能力； 8、提供系统运行状态监测能力，包括运行服务监控、运行服务统计、运行数据报告和运行服务解析概览。 | 套 | 1 | 1、支持管理最大组织数2000个，组织层级最大10级； 2、支持管理最大区域数2000个，区域层级最大10级。； 3、支持管理最大人员数量5万； 4、支持管理最大卡片数量5万； 5、支持管理最大车辆数量3万； 6、支持最大的在线用户数1000个，并发登录用户数50个。 7、支持最大事件并发处理500条/秒（不带图片）； 8、支持联动上墙并发1次/秒； 9、支持最大每秒联动100个不同的视频点位进行抓图； 10、支持最大每秒联动100个不同的视频点位进行录像； 11、支持联动并发发邮件2封/秒； 12、支持短信联动（云信留客短信网关：1-2秒/条； 短信猫：70字符以下，10秒/条； 70字符以上分条发送，20秒/条；） 13、支持最大事件存储7200万条； 14、支持管理资源上图数量2万个。 备注：以上是单台服务器部署系统基础规格，超出规格需考虑分布式部署。 |
| 14 | 视频监控应用提供视频管理服务，支持编码设备通过主流厂商设备无缝兼容现有系统，实现视频预览、录像回放、视频上墙、视频事件监控服务能力，并且在网络带宽不足、有流量限制的网络环境下可以通过以图片替代视频的模式提供监控服务。 一、视频预览 1、支持视频实时预览能力，实现预览窗口布局切换、预览画面自适应及全屏切换； 2、支持云台控制、实时抓图、紧急录像、即时回放、主子码流切换、声音开启\关闭、辅屏预览（1个辅屏）、对讲、广播、报警输出控制的能力； 3、支持智能规则展示的能力（如：针对热成像设备温度信息实时展示）； 4、支持资源视图管理能力，以视图形式管理监控点、视频预览轮巡等自定义资源组，其中视图类型包含公有视图和私有视图； 5、支持全景视频监控预览能力，支持球型鹰眼、全景摄像机的全景模式； 二、录像回放 1、支持录像计划管理能力，支持实时录像计划、录像回传计划； 2、支持录像回放能力，支持多画面同步回放和异步回放切换、超高倍速回放、分段回放、录像下载、录像剪辑、录像标签、录像锁定、录像抓图； 三、图片监控 1、支持视频预览与图片实时监控模式切换能力，实现图片监控模式； 2、支持图片查询回放能力，实现按监控点、时间段展示抓拍图片； 3、支持图片自动播放能力，支持图片自动播放速度可设置； 4、支持图片下载能力； 四、视频上墙 1、支持电视墙场景管理能力，实现场景窗口配置、场景切换计划配置以及轮巡计划的管理； 2、支持上墙控制能力，实现场景一键上墙、场景切换、电视墙切换、监控点上下墙、轮巡控制操作； 五、视频事件 1、支持视频事件布撤防能力，可按计划模版进行布防，事件类型包括移动侦测、视频丢失、视频遮挡、报警输入、报警输出； | 路 | 200 | 1、支持监控点数量10W个（超过5000需要分布式部署）； 2、支持并发取流带宽2000M，例如以2M/路计算最大并发路数为1000路 （以千兆服务器为例，每台服务器并发取流带宽为600M，超过600M需要分布式部署）； 3、解码能力：在i7、GTX1070的PC上，解码H264、720P的视频36路； 4、支持电视墙最大场景数128个； 5、单个电视墙最大支持数量25\*25个； 6、单个窗口最大分割数量16个。 |
| 15 | 设备网络管理应用，对接入平台的视频设备，门禁设备，梯控设备，可视对讲设备进行在线巡检，及时发现故障设备和掉线设备，使运维工作更加高效，便利。 一、视频网络管理 1、支持监控摄像机、编码设备、存储设备、解码设备等物联设备在线状态、工作状态、硬盘状态、指标采集。 2、支持监控点通道的在线状态、录制状态、录像完整性、录像保存天数指标检测。 3、支持告警信息统计展现。并支持对监控点、编码设备、解码设备、视频综合矩阵、NVR/CVR、云储存、门禁设备、门禁点、读卡器、梯控设备/梯控读卡器/可视对讲的告警阈值进行配置。 4、提供视频运维报表统计能力，包含区域综合排名统计、录像完整性统计、录像存储达标统计、在线状态统计、离线时长统计报表。 5、支持巡检计划配置，可以按照类型和资源以及自定义的巡检周期进行巡检计划配置。 6、支持海康SDK、大华SDK、ehome、isup5.0、GB28181、部标808、Open Network Video Interface、萤石、ISAPI协议。 二、门禁运维管理 1、提供门禁设备在线状态监测能力； 2、提供门禁设备运维报表统计能力； 三、可视对讲运维管理 1、提供门口机、室内机、管理机、围墙机设备在线状态监测能力； 2、提供可视对讲设备运维报表统计能力； 四、梯控运维管理 1、提供梯控主机、读卡器在线状态监测能力； 2、提供梯控设备运维报表统计能力； 五、停车场出入口运维管理 1、提供岗亭缴费终端、出入口控制设备、出入口显示设备、读卡设备在线状态监测能力； 2、提供停车场出入口设备运维报表统计能力； 六、寻车诱导运维管理 1、提供诱导管理器、车位相机、显示屏在线状态监测能力； 2、提供寻车诱导设备运维报表统计能力 | 路 | 300 | 1、单节点在线状态巡检效率不低于1000路/小时； 2、单节点录像情况巡检效率不低于1000路/小时 |
| 16 | 提供视频点位联网服务能力，用于平台域间视频联网，基于视频通用标准协议（GB/T28181-2011,GB/T28181-2016）与外域平台互联互通，实现平台视频资源点位推送等操作控制。 1、支持上下级域注册管理能力，实现平台数据级联； 2、支持资源同步能力； 3、支持级联视频点位实时预览、录像回放、录像下载、语音对讲能力； 4、支持级联视频点位设备操作控制能力； | 套 | 1 | 1、最大级联监控点数量20W个； 2、单个NCG信令节点：最大支持5个上级域平台、15个下级域平台； 3、支持并发取流带宽2000M，例如以2M/路计算最大并发路数为1000路 （以千兆服务器为例，每台服务器并发取流带宽为600M，超过600M需要分布式部署）。 |
| 17 | 光模块 | 千兆单模 单芯20KM | 块 | 89 |  |
| 18 | 光模块 | 千兆单模 单芯40KM | 块 | 5 |  |
| 19 | 网线 | 六类非屏蔽网络传输双绞线 | 米 | 5400 | 平均每个点30米 |
| 20 | 光纤跳线 | 2m，SC-LC | 条 | 90 |  |
| 21 | pvc线槽 | 30mm\*15mm\*2mm | 米 | 3600 |  |
| 22 | 电源线 | RVV2\*1.0 | 米 | 600 |  |
| 1. 工期要求：30天 三、服务要求： 2. 针对雁翅镇、清水镇、斋堂镇、王平镇、军庄镇、潭柘寺镇、妙峰山镇、龙泉镇、永定镇管辖内的87个社区卫生室提供服务，包括但不限于提供送货、安装、标识、测试、网线敷设、综合布线、系统调试、培训等集成服务，保证整套系统的正常运转。   2.卫健委机房网络服务器的网络及设备安装布署，要考虑兼容性和匹配性，在保证原有数据的基础上进行系统对接，实现87个卫生室点位与卫生专网接通、实现监控信息与所在属地卫生院联通、所有卫生院实现与卫生健康委联通（含设备配置）等。  3.针对各个卫生室的要求进供培训，指导及使用指南等，提供7\*24小时运维技术支持，确保设备问题能够及时解决服务。提供定期上门巡检服务，确保设备正常运行。监控信息至少保存3个月及以上。设备质保期36个月。 | | | | | |